17. Tätigkeitsbericht

der Beauftragten für den Datenschutz

des

Rundfunk Berlin-Brandenburg

Berichtszeitraum:

1. April 2020 bis 31. März 2021

Dem Rundfunkrat gemäß § 38 Abs. 7 rbb-Staatsvertrag

vorgelegt von

Anke Naujock-Simon

Inhaltsverzeichnis

Abkürzungsverzeichnis

AK DSB	Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio
ARD-GS	ARD-Generalsekretariat
BDSG	Bundesdatenschutzgesetz
BGH	Bundesgerichtshof
BfDI	Bundesbeauftragter für Datenschutz und Informationsfreiheit
BlnBDI	Berliner Beauftragte für Datenschutz und Informationsfreiheit
BlnDSG	Berliner Datenschutzgesetz
BND-Gesetz	Bundesnachrichtendienst-Gesetz
BSI	Bundesamt für Sicherheit in der Informations-Technik
CC ISec	Corporation Center Information Security (Zusammenschluss der Informationssicherheitsbeauftragten von ARD, ZDF und DLR)
BVerfG	Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht
DA	Dienstanweisung
DLR	Deutschlandradio
DSFA	Datenschutz-Folgenabschätzung
DSGVO	EU-Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
EDSA	Europäischer Datenschutz-Ausschuss
EG	Erwägungsgrund
EMS	Eletronic Media School

EU	Europäische Union
EuGH	Europäischer Gerichtshof
FSZ	Fernsehzentrum
GG	Grundgesetz
GeschGehG	Geschäftsgeheimnisgesetz
GRCh	Charta der Grundrechte der Europäischen Union
GO	Geschäftsordnung
HA	Hauptabteilung
HA MIT	Hauptabteilung Mediensysteme und IT
HdR	Haus des Rundfunks
HSB	ARD-Hauptstadtstudio
IVZ	Informationsverarbeitungszentrum
JuKo	Juristische Kommission
KEF	Kommission zur Ermittlung des Finanzbedarfs der Rundfunkanstalten
KI	Künstliche Intelligenz
LG	Landgericht
MÄndStV	Medienänderungsstaatsvertrag
MIT	Mediensysteme und IT
MStV	Medienstaatsvertrag
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
POC	Proof of Concept
OTT-Dienste	Over-The-Top-Dienste
RÄndStV	Rundfunkänderungsstaatsvertrag
rbb-StV	Staatsvertrag über die Errichtung einer gemeinsamen Rundfunkanstalt der Länder Berlin und Brandenburg (rbb-Staatsvertrag)
RBStV	Rundfunkbeitragsstaatsvertrag
RDSK	Rundfunkdatenschutzkonferenz

RStV	Rundfunkstaatsvertrag
SolMan	Solution Manager
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TTDSG	Telekommunikation-Telemedien-Datenschutzgesetz
UC	Unified Communication
VG	Verwaltungsgericht
VVT	Verzeichnis von Verarbeitungstätigkeiten
ZBS	Zentraler Beitragsservice

Vorbemerkung

Mit diesem Tätigkeitsbericht wird die Entwicklung des Datenschutzes beim Rundfunk Berlin-Brandenburg (rbb) für die Zeit vom 1.4.2020 bis 31.3.2021 dokumentiert. Der Tätigkeitsbericht umfasst meine Aktivitäten als Beauftragte für den Datenschutz im journalistisch-redaktionellen Bereich und als betriebliche Datenschutzbeauftragte im wirtschaftlich-administrativen Bereich.

Im Berichtszeitraum war meine Arbeit stark von den Corona-bedingten Abstandsregelungen geprägt. Die Zusammenarbeit mit den rbb-Kolleg:innen, der Austausch mit den Datenschutzbeauftragten der anderen Rundfunkanstalten, die Teilnahme an Seminaren und vieles mehr fand überwiegend per Videokonferenz statt. Diese virtuelle Zusammenarbeit war zunächst ungewohnt. Schnell wurden aber die Vorteile erkennbar. Die Möglichkeiten, zeitlich und örtlich flexibel zu arbeiten, Reisezeiten einzusparen und gemeinsam an elektronischen Dokumenten zu arbeiten, werde ich auch nach Überwindung der Pandemie nicht mehr missen wollen. Andererseits fehlt mir die gemeinsame Arbeit vor Ort und der informelle Austausch bei einer gemeinsamen Tasse Kaffee oder einem gemeinsamen Spaziergang während der Mittagspause. Reale Begegnungen halte ich für eine effektive Zusammenarbeit auf Dauer für unersetzlich.

Angesichts der Fülle der im Berichtsjahr bearbeiteten Fragestellungen muss sich auch der diesjährige Bericht wieder auf die wesentlichen Themen beschränken.

Inhaltlich stand die datenschutzrechtliche Prüfung weiterer ‚Tools' aus dem ‚Werkzeugkasten' von Microsoft 365 im Vordergrund. Außerdem habe ich viele weitere größere und kleinere Projekte datenschutzrechtlich begleitet und war mit zahlreichen Einzelfragen befasst.

Mit Sorge ist zu konstatieren, dass der rbb, wie alle anderen ARD-Anstalten, nach und nach Teile seiner digitalen Souveränität aufgibt und seine Daten in Clouds auslagert. Neben Aspekten der Benutzerfreundlichkeit (‚Usability') dürfte in vielen Fällen vor allem die Wirtschaftlichkeit der Hintergrund hierfür sein. Die Datenschutzbeauftragte hat diese unternehmenspolitischen Entscheidungen zu respektieren. Allerdings achtet sie bei diesem Prozess ganz

besonders darauf, dass die Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten gewahrt bleiben.

Ich danke meinem ehemaligen Assistenten Herrn Christoph Schneider und meiner aktuellen Assistentin Frau Ulrike Stephan für ihr Engagement und ihre tatkräftige Unterstützung im Berichtsjahr. Dank gebührt auch in diesem Jahr wieder meinem Stellvertreter Herrn Axel Kauffmann, der mich in Abwesenheitsfällen stets zuverlässig und fachkundig vertreten hat. Die konstruktive Zusammenarbeit mit dem Informationssicherheitsbeauftragten Herrn Michael Kalisch und seinem Mitarbeiter Herrn Marcel Kuring konnte im Berichtsjahr weiter ausgebaut und vertieft werden. Auch ihnen danke ich sehr.

Schließlich danke ich der Intendantin und allen weiteren Mitgliedern der Geschäftsleitung für ihr Vertrauen in meine Arbeit und ihre umfassende Unterstützung.

Dieser Tätigkeitsbericht wird – wie alle Vorgängerberichte – im Online-Angebot des rbb veröffentlicht, abrufbar unter:

http://www.rbb-online.de/unternehmen/der_rbb/struktur/datenschutz/datenschutz_im_rbb.html

A. Die Stellung der Beauftragten für den Datenschutz des Rundfunk Berlin-Brandenburg

I. Gesetzliche Grundlagen

Gemäß § 38 Abs. 1 rbb-Staatsvertrag (rbb-StV) bestellt der Rundfunkrat einen Beauftragten oder eine Beauftragte für den Datenschutz. Er/Sie ist in Ausübung dieses Amtes unabhängig und nur dem Gesetz unterworfen und untersteht im Übrigen der Dienstaufsicht des rbb-Verwaltungsrates.

Gemäß Abs. 2 Satz 2 überwacht er/sie die Einhaltung der Datenschutzvorschriften des rbb-StV und anderer Vorschriften über den Datenschutz, soweit der rbb personenbezogene Daten zu eigenen journalistisch-redaktionellen oder literarischen Zwecken verarbeitet.

Soweit eine Befugnis des oder der Beauftragten für den Datenschutz nach Abs. 2 Satz 1 nicht gegeben ist, obliegt die Kontrolle der Einhaltung von Datenschutzbestimmungen beim rbb dem oder der Landesbeauftragten für den Datenschutz des Landes Berlin. Die Kontrolle erfolgt im Benehmen mit dem oder der Landesbeauftragten des Landes Brandenburg (Abs. 8).

Für die Sicherstellung des Datenschutzes im wirtschaftlich-administrativen Bereich ist beim rbb außerdem – wie bei allen Berliner Behörden und sonstigen öffentlich-rechtlichen Stellen – ein/e betriebliche/r Datenschutzbeauftragte/r sowie jeweils ein/e Stellvertreter/in zu bestellen. Diese Pflicht ergibt sich aus § 36 Abs. 1 rbb-StV i. V. m. § 4 Abs. 1 des Berliner Datenschutzgesetzes (BlnDSG).

Die Aufgaben und Befugnisse der Rundfunkdatenschutzbeauftragten werden durch Art. 51 ff. EU-Datenschutzgrundverordnung (DSGVO) konkretisiert. Gemäß Art. 57 DSGVO haben die datenschutzrechtlichen Aufsichtsbehörden – und damit auch die rbb-Datenschutzbeauftragte im journalistisch-redaktionellen Bereich – u. a. folgende Aufgaben:

- Überwachung der Einhaltung der DSGVO
- Beratung, Aufklärung und Sensibilisierung der Verantwortlichen und der Öffentlichkeit für die Risiken im Zusammenhang mit der Verarbeitung von personenbezogenen Daten
- Bearbeitung von Datenschutzbeschwerden
- Zusammenarbeit mit den anderen datenschutzrechtlichen Aufsichtsbehörden
- Erstellung eines jährlichen Tätigkeitsberichts.

Nach Art. 39 DSGVO hat der/die betriebliche Datenschutzbeauftragte – und damit auch die rbb-Datenschutzbeauftragte im wirtschaftlich-administrativen Bereich – mindestens folgende Aufgaben zu erfüllen:

- Unterrichtung und Beratung der Verantwortlichen und der Beschäftigten, die Datenverarbeitungen durchführen, hinsichtlich ihrer Pflichten nach der DSGVO sowie der sonstigen Datenschutzvorschriften
- kontinuierliche Überwachung der Einhaltung der datenschutzrechtlichen Bestimmungen sowie der Strategien der Verantwortlichen für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Beschäftigten und diesbezügliche Überprüfungen
- Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung (DSFA) und Überwachung ihrer Durchführung
- Zusammenarbeit mit der Aufsichtsbehörde als Ansprechpartnerin in Fragen der Verarbeitung personenbezogener Daten, einschließlich der vorherigen Konsultation gemäß Art. 36 DSGVO und gegebenenfalls Beratung zu allen sonstigen Fragen.

Die Gegenüberstellung der Aufgaben der Aufsichtsbehörde und der betrieblichen Datenschutzbeauftragten, deren Kompetenzen durch die DSGVO erweitert wurden („Überwachung“, anstatt wie zuvor „Hinwirken auf die Einhaltung der Datenschutzgesetze“), zeigt viele Überschneidungen. Das bedeutet für die Datenschutzbeauftragte des rbb, dass es bei

der täglichen Arbeit kaum einen Unterschied macht, ob sie in der einen oder anderen Funktion tätig wird, zumal sie oftmals auch im wirtschaftlich-administrativen Bereich von den Mitarbeiter:innen und Geschäftspartner:innen als erste Anlaufstelle für datenschutzrechtliche Beschwerden gesehen wird.

Die speziellen Aufgaben der rbb-Datenschutzbeauftragten sind zudem in Anlage 2 ‚Datenschutz' der Dienstanweisung Informationsmanagement beschrieben.

II. Konkrete Situation

Auf seiner Sitzung am 20.6.2019 hat mich der Rundfunkrat gemäß § 38 Abs. 1 rbb-StV auf Vorschlag der Intendantin für eine weitere Amtszeit von vier Jahren für den Zeitraum 1.7.2019 bis 30.6.2023 zur Beauftragten für den Datenschutz bestellt. Parallel dazu hat mich die Intendantin für den gleichen Zeitraum zur betrieblichen Datenschutzbeauftragten gemäß § 4 Abs. 1 BlnDSG ernannt. Ich nehme die Funktion der Rundfunkdatenschutzbeauftragten gemäß § 38 Abs. 1 rbb-StV und der betrieblichen Datenschutzbeauftragten gemäß § 4 BlnDSG hauptamtlich und in Personalunion wahr. Zusätzlich bekleide ich seit 1.7.2019 das Amt der Compliance-Beauftragten.

Seit dem 1.4.2014 ist der Leiter der Innenrevision, Herr Axel Kauffmann, stellvertretender betrieblicher Datenschutzbeauftragter. Herr Kauffmann vertritt mich in Abwesenheitsfällen. Zusätzlich hat er auch in diesem Berichtszeitraum wieder eine Reihe von Datenschutzschulungen durchgeführt.

Anfang 2021 ist mein bisheriger Assistent, Herr Christoph Schneider, in den Verwaltungsbereich des ARD-Hauptstadtstudios gewechselt. Seitdem unterstützt mich Frau Ulrike Stephan bei den Sekretariats- und Sachbearbeitungstätigkeiten.

Seit Juli 2020 bildet die rbb-Datenschutzbeauftragte Rechtsreferendar:innen aus. Die Entscheidung hierfür hat sich als richtig erwiesen: Die Ausbildung ist aufgrund der gewachsenen Bedeutung des Datenschutzrechts sehr nachgefragt und kommt beiden Seiten zugute.

B. Entwicklung des Datenschutzrechts

I. Europa

1. Verordnungen und Richtlinien

1.1. EU-Datenschutzgrundverordnung

Seit dem 25.5.2018 ist die DSGVO in allen Mitgliedsstaaten der Europäischen Union direkt geltendes Recht. Nach einer Evaluation hat das EU-Parlament mit Entschließung vom 25.3.2021 festgestellt, dass die Bestimmungen der DSGVO nach dreijähriger Geltungsdauer insgesamt positiv zu bewerten sind und einen Erfolg für Europa darstellen. Das EU-Parlament und die EU-Kommission sehen derzeit keinen Überarbeitungsbedarf. Nachbesserungsbedarf hat das EU-Parlament jedoch im Hinblick auf eine effektivere Durchsetzung bei Ansprüchen von Betroffenen sowie hinsichtlich einer ausreichenden personellen, technischen und finanziellen Ausstattung für die Aufsichtsbehörden festgestellt.

Für Auslegungsfragen sind vor allem die Arbeit des Europäischen Datenschutzausschusses (EDSA) und die Rechtsprechung des Europäischen Gerichtshofs (EuGH) maßgeblich.
Der EDSA besteht aus der Leitung einer Aufsichtsbehörde jedes Mitgliedsstaates und dem/der Europäischen Datenschutzbeauftragten (Art. 68 Abs. 3 DSGVO). Ist in einem Mitgliedsstaat mehr als eine Aufsichtsbehörde für die Überwachung der Anwendung der nach Maßgabe der DSGVO erlassenen Vorschriften zuständig, so wird im Einklang mit den Rechtsvorschriften dieses Mitgliedsstaates ein Gemeinsamer Vertreter benannt (Art. 68 Abs. 4 DSGVO). § 17 Abs. 1 Bundesdatenschutzgesetz (BDSG) legt fest, dass die Funktion des Gemeinsamen Vertreters der deutschen Aufsichtsbehörden im EDSA von dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) wahrgenommen wird. Als Stellvertreter des Gemeinsamen Vertreters ist vorgesehen, dass der Bundesrat eine Leiterin oder einen Leiter einer Aufsichtsbehörde der Länder wählt. Dieser gesetzlichen Verpflichtung ist der Bundesrat bisher nicht nachgekommen. Die Aufsichtsbehörden der Länder haben den Hamburgischen Datenschutzbeauftragten mit der Wahrnehmung ihrer Interessen im EDSA betraut, solange der Bundesrat keine/n Stellvertreter/in gewählt hat. Die vom EDSA veröffentlichten Papiere sind für die Praxis nach Einschätzung der Datenschutzbeauftragten derzeit nur bedingt hilfreich, zumal

sie ihrerseits in vielen Fällen von den Aufsichtsbehörden der Mitgliedsstaaten unterschiedlich interpretiert werden.

1.2. ePrivacy-Verordnung

Die ePrivacy-Verordnung soll Vorgaben zum Datenschutz bei der Bereitstellung und Nutzung von Telemediendiensten, klassischen Kommunikationsdiensten wie Telefonie und SMS und internetbasierten Kommunikationsdiensten, insbesondere Messenger wie Skype oder WhatsApp regeln. Ursprünglich sollte sie zeitgleich mit der DSGVO in Kraft treten. Über den Stand des Verordnungsentwurfs habe ich in der Vergangenheit wiederholt berichtet (zuletzt 16. Tätigkeitsbericht, S. 14). Im Rahmen ihrer Präsidentschaft (1.7.2020 bis 31.12.2020) hatte die Bundesrepublik Deutschland im EU-Ministerrat versucht, mit einem eigenen Vorschlag die Verhandlungen erfolgreich zum Abschluss zu bringen. Dieser Versuch scheiterte ebenso wie mehrere andere Versuche zuvor. Im Februar 2021 hat sich der EU-Ministerrat nun unter dem Vorsitz von Portugal auf einen neuen Entwurf geeinigt. Dieser bleibt aus Datenschutzsicht hinter den bisherigen Entwürfen zurück. Denn er sieht vor, dass Metadaten von Nutzenden verarbeitet werden dürfen, wenn es dafür „kompatible Gründe“ gibt. Außerdem sind darin weitreichende Ausnahmen vom Einwilligungserfordernis beim Setzen von Cookies enthalten. Aktuell finden die sogenannten Trilog-Verhandlungen statt. Der Trilog ist ein paritätisch zusammengesetztes Dreiertreffen der gesetzgebenden Institutionen der EU, der EU-Kommission, des EU-Ministerrats und des EU-Parlaments. Mit der Verabschiedung der ePrivacy-Verordnung ist realistisch nicht vor 2024 zu rechnen.

Auf nationaler Ebene läuft zeitgleich das Gesetzgebungsverfahren für ein Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG) mit zum Teil deckungsgleichen Regelungsgegenständen. Die im vorliegenden Entwurf für das TTDSG enthaltenen Vorgaben für das Setzen von Cookies sind gegenüber den Regelungen im aktuellen Entwurf der ePrivacy-Verordnung wesentlich restriktiver (s. dazu II. 1.2.).

1.3. Brexit

Zum 31.1.2020 ist Großbritannien aus der EU ausgetreten. Obwohl das Vereinigte Königreich damit seit dem 1.2.2020 zu einem „Drittland“ im datenschutzrechtlichen Sinne geworden ist, konnten bis zum 31.12.2020 zunächst weiterhin ohne besondere zusätzliche Schutzmaßnahmen personenbezogene Daten nach Großbritannien übermittelt werden. Denn das Austrittsabkommen zwischen der EU und Großbritannien legte fest, dass die DSGVO in einem Übergangszeitraum bis zum 31.12.2020 weiterhin auch in Großbritannien galt. In der gemeinsamen politischen Erklärung zum zukünftigen Verhältnis zwischen der EU und Großbritannien wurde zudem vereinbart, dass die EU-Kommission bis zum Ende des Übergangszeitraums entsprechende Angemessenheitsbeschlüsse erlässt, was bislang aber nicht geschehen ist.

Am 24.12.2020 haben sich die EU und Großbritannien auf einen sogenannten ‚Brexit-Deal‘ geeinigt. Danach ist der freie Datenfluss zwischen der EU und Großbritannien für weitere vier Monate (also bis einschließlich April 2021), verlängerbar bis Ende Juni 2021, ohne weiteres zulässig. Die Rundfunkanstalten müssen die weiteren Entwicklungen im Auge behalten, da sie insbesondere im technischen Bereich auch mit Dienstleistern aus Großbritannien zusammenarbeiten. Falls nicht rechtzeitig ein Angemessenheitsbeschluss der EU-Kommission vorliegt, muss ersatzweise zivilrechtlich durch den Abschluss von Standardvertragsklauseln mit den Dienstleistern vereinbart werden, dass in der Zusammenarbeit das Europäische Datenschutzniveau gewahrt bleibt (zu den Standardvertragsklauseln s. auch 2.1.4.).

1.4. Richtlinie über Maßnahmen für ein hohes gemeinsames Niveau der Cybersicherheit in der gesamten Union

Am 14.12.2020 hat der EU-Ministerrat eine Entschließung zur Verschlüsselung von elektronischem Datenverkehr verabschiedet: „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“. In dieser Entschließung hebt er einerseits seine Unterstützung für die Entwicklung, Umsetzung und Nutzung starker Verschlüsselung als einem notwendigen Mittel zum Schutz der Grundrechte und der digitalen Sicherheit der Bürgerinnen und Bürger hervor.

Andererseits betont er, dass gewährleistet werden muss, dass die Strafverfolgungs- und Justizbehörden ihre gesetzlichen Befugnisse auch online ausüben können, um die Gesellschaft sowie Bürgerinnen und Bürger zu schützen.

Die Strafverfolgungsbehörden und die Justiz seien zunehmend auf den Zugang zu elektronischen Beweismitteln angewiesen, um Terrorismus, organisierte Kriminalität, sexuellen Missbrauch von Kindern sowie eine Reihe anderer Cyberstraftaten und durch den Cyberraum ermöglichter Straftaten wirksam zu bekämpfen. Technische Lösungen müssten es den Behörden ermöglichen, ihre Untersuchungsbefugnisse auszuüben, die nach innerstaatlichem Recht dem Gebot der Verhältnismäßigkeit und der gerichtlichen Kontrolle unterliegen, wobei die gemeinsamen europäischen Werte und die Grundrechte zu achten und die Vorteile der Verschlüsselung zu wahren seien. Auf dieser Basis hat die EU Kommission am 16.12.2020 den Entwurf einer Richtlinie über Maßnahmen für ein hohes gemeinsames Niveau der Cybersicherheit in der gesamten Union veröffentlicht. Danach soll für Strafverfolgungsbehörden und Justiz auch die Möglichkeit des Zugriffs auf den verschlüsselten Datenverkehr möglich sein. Die Rundfunkanstalten werden bei dem weiteren Verfahren darauf zu achten haben, dass der Informantenschutz beim elektronischen Datenaustausch trotz dieser Bestrebungen gewahrt bleibt.

2. Entscheidungen

2.1 EuGH-Urteil zum Privacy Shield (‚Schrems II')

2.1.1. Das Urteil

Die Übermittlung von personenbezogenen Daten in Drittstaaten darf grundsätzlich nur dann erfolgen, wenn in diesen Drittstaaten ein Datenschutzniveau gewährleistet werden kann, das dem der DSGVO gleichwertig ist. Dies kann die EU-Kommission in einem sogenannten Angemessenheitsbeschluss feststellen.

Nachdem der EuGH in seinem Urteil vom 6.10.2015 den ursprünglichen Angemessenheitsbeschluss der EU-Kommission für die USA und die dem Beschluss zugrundeliegende Safe-Harbor-Regelung für unwirksam erklärt hatte (sog. ‚Schrems I'-Urteil, benannt nach dem

österreichischen Kläger und Datenschutzaktivisten Max Schrems), hatten die EU und die USA ein neues Abkommen, den sogenannten EU-US-Datenschutzschild (Privacy Shield) geschlossen. Auf dieser Grundlage hat die EU-Kommission im Jahr 2016 erneut einen Angemessenheitsbeschluss gefasst und die Feststellung der Angemessenheit in ihren jährlichen Überprüfungen wiederholt bestätigt (s. dazu auch mein 16. Tätigkeitsbericht, S. 15 und 21 ff.). Diesen auf den Privacy Shield gestützten Angemessenheitsbeschluss hat der EuGH mit Urteil vom 16.7.2020 (C-311/18) für ungültig erklärt (sog. ‚Schrems II'- Urteil).

Für das Gericht war ausschlaggebend, dass in den USA weitreichende Zugriffsmöglichkeiten der Behörden auf die Daten von EU-Bürger:innen bestehen. Das US-Recht ermächtigt amerikanische Behörden zur Durchführung von Überwachungsmaßnahmen zum Zweck der Auslandsaufklärung ohne jegliche Einschränkungen und Rechtsschutzgarantien. Dadurch werden die europarechtlichen Grundrechte und Rechtsschutzmechanismen unterlaufen. Ein derartiger Eingriff in den Schutzbereich der personenbezogenen Daten ohne eine gesetzlich geregelte legitime Grundlage, die klare und präzise Regeln für die Tragweite und Anwendung der betreffenden Maßnahme vorsieht, trage dem Grundsatz der Verhältnismäßigkeit keineswegs Rechnung und widerspreche damit Art. 8 Abs. 2 in Verbindung mit Art. 52 Abs. 1 Satz 1 der Charta der Grundrechte der Europäischen Union (GRCh). Zudem sei den amerikanischen Nachrichtendiensten eine Sammelerhebung von personenbezogenen Daten mittels entsprechender Überwachungsprogramme erlaubt, ohne die Maßnahme dabei hinreichend klar und präzise zu regeln und einer gerichtlichen Kontrolle zu unterwerfen. Die zugrunde liegende Regelung räume den betroffenen EU-Bürger:innen auch keinen entsprechenden Rechtsschutz gegen derartige Überwachungsmaßnahmen ein und verstoße damit gegen das in Art. 47 GRCh normierte Rechtsschutzgebot.

In seiner Entscheidung setzt sich der EuGH auch mit der Zulässigkeit der sogenannten Standardvertragsklauseln auseinander. Diese seien zwar grundsätzlich zulässig. Aufgrund der Tatsache, dass die zivilrechtlichen Standarddatenschutzklauseln keine drittstaatlichen Behörden binden können, reiche der bloße Vertragsschluss allerdings nicht aus, um ein europäisches Datenschutzniveau zu gewährleisten. Es bedürfe daher vielmehr zusätzlicher Maßnahmen.

Nachdem folglich auch die Standardvertragsklauseln für die Datenübermittlung an US-amerikanische Vertragspartner allein kein geeignetes Instrument mehr darstellen, ist die Frage nach Alternativen für die Praxis bedeutsam. Der EuGH stellt dabei ausdrücklich auf die in Art. 49 DSGVO geregelten Erlaubnistatbestände zur Datenübermittlung an Drittstaaten ab, sofern weder ein Angemessenheitsbeschluss nach Art. 45 Abs. 3 DSGVO vorliegt noch geeignete Garantien im Sinne von Art. 46 DSGVO bestehen, was dem Urteil nach in Bezug auf einen Datentransfer in die USA der Fall ist. Art. 49 DSGVO erlaubt den Transfer von personenbezogenen Daten in einen Drittstaat unter anderem aufgrund einer ausdrücklichen Einwilligung, zur Durchführung eines Vertrages oder bei Vorliegen wichtiger Gründe des öffentlichen Interesses.

Allerdings dürfte Art. 49 DSGVO als Rechtsgrundlage für die Praxis eine unbefriedigende Lösung darstellen. Beispielsweise ist die Einholung einer Einwilligung von Beschäftigten eines in Deutschland ansässigen Unternehmens für die Datenübermittlung im Zusammenhang mit der Nutzung von US-amerikanischen Cloud-Diensten keine geeignete Lösung, weil sie mangels Freiwilligkeit unwirksam sein dürfte. Des Weiteren ist im Hinblick auf die Konzeption des Art. 49 DSGVO als Ausnahmetatbestand eine restriktive Auslegung der Vorschrift geboten. Die Datenübermittlung darf nur gelegentlich erfolgen. Insofern wird Art. 49 DSGVO in der Praxis für Unternehmen und vor allem auch für die Rundfunkanstalten nicht als Erlaubnistatbestand für die Übermittlung von Daten in die USA fungieren können, wenn die Datenübertragung im Rahmen einer auf Dauer angelegten Nutzung von amerikanischen Cloud-Diensten, wie Microsoft 365 oder ähnlichen Dienstleistungen aus den USA erfolgt.

2.1.2. Empfehlungen der RDSK zur Umsetzung des ‚Schrems II'-Urteils

Die Rundfunkdatenschutzkonferenz (RDSK) hat im August 2020 ein Empfehlungspapier zum weiteren Vorgehen nach ‚Schrems II' verfasst (Anlage 1). Danach sollen die Rundfunkanstalten im ersten Schritt eine Bestandsaufnahme der Datenübermittlung in die USA durchführen. Es muss eine Neubewertung der jeweiligen Datenverarbeitung hinsichtlich ihrer Art, ihres Umfangs, des Zwecks der Verarbeitung sowie der vorgesehenen Empfänger stattfinden. Maßgeblich für die Bewertung muss dabei der risikobasierte Ansatz sein, der die DSGVO prägt. Im

Hinblick auf die zu ergreifenden Maßnahmen kommt es u. a. darauf an, ob nur wenige und vergleichsweise unkritische Daten in den USA verarbeitet werden. Bei Verwendung der Standardvertragsklauseln soll der Empfänger der Daten aufgefordert werden zuzusichern, die Rundfunkanstalt über einen etwaigen Zugriff durch die US-Behörden zu informieren und gegen unverhältnismäßige Zugriffe rechtlich vorzugehen. Zu prüfen ist außerdem, ob durch geeignete technische und ggf. auch organisatorische Maßnahmen ein Zugriff der US-Behörden verhindert werden kann. Hier kommen insbesondere wirksame Verschlüsselungstechniken wie Ende-zu-Ende-Verschlüsselungen in Betracht. Innerhalb des rbb dauert diese Bestandsaufnahme – wie auch in den anderen Rundfunkanstalten – noch an.

2.1.3. Empfehlungen des EDSA zu Datentransfers nach ‚Schrems II'

Anknüpfend an die vom EuGH festgestellte Notwendigkeit, in Ergänzung zu den Standardvertragsklauseln zusätzliche Maßnahmen zu treffen, hat der EDSA am 10.11.2020 entsprechende Empfehlungen vorgelegt. Die Hoffnungen, dass diese Empfehlungen verlässliche Lösungen bringen würden, wurden im Ergebnis enttäuscht, denn es handelt sich nicht um klar umsetzbare Vorgaben. Vielmehr werden auf 38 Seiten Probleme, Vorschläge und Ideen vorgestellt – verbunden mit dem Hinweis, dies selbst auf jeden Einzelfall anzuwenden und angemessene Lösungen zu finden.

2.1.4. Empfehlungen der EU-Kommission zur Überarbeitung der Standardvertragsklauseln

Am 12.11.2020, nur einen Tag, nachdem der EDSA seine Empfehlungen zu Datentransfers veröffentlicht hatte (s. 2.1.3.), hat die EU-Kommission als Reaktion auf das ‚Schrems II'-Urteil des EuGH einen Entwurf zur Überarbeitung der Standardvertragsklauseln vorgelegt. In den Entwurf sind neue Garantien für den Transfer personenbezogener Daten außerhalb der EU aufgenommen worden. So soll sich der Datenimporteur (der außereuropäische Vertragspartner)

verpflichten, Betroffene bei Behördenanfragen zu benachrichtigen und zur Vermeidung der Erteilung der Auskunft im äußersten Fall alle verfügbaren Rechtsmittel auszuschöpfen.

Es finden nun zunächst umfangreiche Anhörungen und Konsultationen zu dem Entwurf statt, bevor die neuen Standardvertragsklauseln von der EU-Kommission erlassen werden können.

2.2. EuGH-Urteil zur Vorratsdatenspeicherung

Der EuGH hat am 6.10.2020 in seinen Urteilen zu drei Klagen (Vorlagen aus Großbritannien, Frankreich und Belgien) erneut festgestellt, dass eine flächendeckende und pauschale Speicherung von Internet- und Telefonverbindungsdaten auf Vorrat nicht zulässig ist. Ausnahmen seien aber möglich, wenn es um die Bekämpfung schwerer Kriminalität oder um die Bedrohung der nationalen Sicherheit gehe. Bereits in den Jahren 2014 und 2016 hatte der EuGH in entsprechenden Urteilen die Vorratsdatenspeicherung weitgehend für nicht vereinbar mit EU-Grundrechten befunden. Den vorlegenden Ländern ging es um die Klärung der Frage, ob die Vorratsdatenspeicherung ausnahmsweise für Terrorismusbekämpfung eingesetzt werden könne. Mit den Entscheidungen bekräftigt der EuGH seine grundsätzlich ablehnende Haltung zur Vorratsdatenspeicherung, entwickelt sie aber auch weiter. Zu dem generellen Verbot der Vorratsdatenspeicherung hat er nun Ausnahmen definiert. Danach bleibt es den nationalen Gesetzgebern möglich, eine Vorratsdatenspeicherung unter strengen Voraussetzungen einzuführen. Allerdings darf die Bevorratung und Übermittlung der Daten von Internetanbietern an die Sicherheitsbehörden nur für einen begrenzten Zeitraum vorgesehen werden. Und sie darf nur in engen Verhältnismäßigkeitsgrenzen stattfinden. Der Grundrechtseingriff muss auch einer gerichtlichen Kontrolle unterliegen.

In Deutschland ist im Jahr 2015 das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten eingeführt worden. Gespeichert werden sollen danach Verbindungsdaten – etwa Angaben dazu, wer wann mit wem telefonierte und in welcher Handy-Funkzelle er sich aufhielt. Das Gesetz sieht eine Speicherfrist von zehn Wochen vor. Die Vorratsdatenspeicherung sollte nach dem Gesetz ab 1.7.2017 beginnen. Nach einer Entscheidung des Oberverwaltungsgerichts (OVG) Nordrhein-Westfalen wurde sie Ende Juni 2017

jedoch zunächst ausgesetzt. Nachdem das Bundesverwaltungsgericht (BVerwG) durch Sprungrevision in zwei Verfahren mit dem Gesetz befasst wurde, legte es mehrere Rechtsfragen dazu Ende 2019 dem EuGH vor. Auch dem BVerwG geht es um eine Klärung, ob es Ausnahmen vom generellen Verbot der Vorratsdatenspeicherung geben kann. Über die Vorlage des BVerwG hat der EuGH noch nicht entschieden. Gegen das deutsche Gesetz sind auch beim Bundesverfassungsgericht (BVerfG) Beschwerden anhängig.

Am 6.11.2020 hat der Wissenschaftliche Dienst des Bundestages eine Ausarbeitung zu den Auswirkungen der EuGH-Rechtsprechung auf das deutsche Gesetz aus dem Jahr 2015 veröffentlicht. Er kommt zu dem Ergebnis, dass dieses Gesetz den Anforderungen der EuGH-Rechtsprechung nicht gerecht wird. Ungeachtet dessen findet sich die Verpflichtung zur Vorratsdatenspeicherung nahezu unverändert auch im Entwurf des Telekommunikationsmodernisierungsgesetzes (s. II. 1.3.).

II. Bund

1. Gesetze

1.1. Gesetz zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des BVerfG vom 27.5.2020

Seit 1.4.2021 ist das Gesetz zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des BVerfG vom 27.5.2020 in Kraft. Damit wurden sowohl § 113 Telekommunikationsgesetz (TKG) als auch diejenigen Normen einschränkend konkretisiert, die den Abruf dieser Daten durch verschiedene Sicherheitsbehörden des Bundes, wie etwa durch das Bundeskriminalamt, die Bundespolizei und durch das Bundesamt für Verfassungsschutz regeln.

Das BVerfG hatte zuvor in seinem Urteil vom 27.5.2020 diese Normen für teilweise verfassungswidrig erklärt („Bestandsdatenauskunft II“, Az. 1 BvR 1873/13 und 1 BvR 2618/13). § 113 TKG berechtigt Anbieter von Telekommunikationsdiensten zur Übermittlung von Bestandsdaten im sogenannten manuellen Auskunftsverfahren. Die weiteren mit der

Verfassungsbeschwerde angegriffenen Normen regeln den Abruf dieser Daten durch verschiedene Sicherheitsbehörden des Bundes. Alle angegriffenen Regelungen sollten der Umsetzung der Entscheidung des BVerfG vom 24. 1.2012 (1 BvR 1299/05 „Bestandsdatenauskunft I“) dienen, mit der § 113 TKG in seiner damaligen Fassung teilweise für verfassungswidrig erklärt und das Fehlen fachrechtlicher Abrufregelungen beanstandet worden war.

Nach Auffassung des BVerfG ist die Erteilung einer Auskunft über Bestandsdaten grundsätzlich verfassungsrechtlich zulässig. Der Gesetzgeber müsse aber „nach dem Bild einer Doppeltür“ sowohl für die Übermittlung der Bestandsdaten durch die Telekommunikationsanbieter als auch für den Abruf dieser Daten durch die Behörden jeweils verhältnismäßige Rechtsgrundlagen schaffen. Die in § 113 Abs. 1 Satz 1 TKG a. F. geregelte allgemeine Bestandsdatenauskunft stellte einen Eingriff in das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz (GG) dar und wies diesbezüglich keine begrenzenden Eingriffsschwellen auf. Vielmehr ermöglichte die Vorschrift anlasslose Auskünfte, die bereits dann erteilt werden könnten, wenn sie in irgendeinem Zusammenhang zur staatlichen Aufgabenwahrnehmung stehen. Die mit § 113 TKG korrespondierenden Abrufregelungen spezialgesetzlicher Regelungen, welche den Abruf der von den Telekommunikationsanbietern erhobenen Daten durch die Sicherheitsbehörden bestimmen (z. B. BND-Gesetz, Bundespolizeigesetz u. a.), genügten im Wesentlichen ebenfalls nicht den verfassungsrechtlichen Anforderungen, da sie ebenfalls keine begrenzenden Eingriffsschwellen beinhalteten, sondern den Abruf generell zur Wahrnehmung der jeweiligen behördlichen Aufgaben erlaubten.

Diesen Feststellungen hat der Gesetzgeber mit Gesetz zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des BVerfG vom 27.5.2020 nun Rechnung getragen.

1.2. Entwurf eines Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien

Am 10.2.2021 hat die Bundesregierung einen Gesetzentwurf zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG)

beschlossen. Ziel des Gesetzentwurfs ist es, die bisherigen datenschutzrechtlichen Bestimmungen des TKG und des Telemediengesetzes (TMG) aus diesen Gesetzen auszugliedern und zusammenzuführen. Außerdem soll damit die erforderliche Anpassung der Datenschutzbestimmungen an die DSGVO sowie die rechtssichere Umsetzung der Regelung zum Schutz der Privatsphäre in Endeinrichtungen in der vor der Ablösung stehenden ePrivacy-Richtlinie in nationales Recht erfolgen. Bei den Regelungen zur Rechtmäßigkeit der Speicherung von Daten in Endeinrichtungen (insbesondere von Cookies) orientiert sich der Gesetzentwurf eng an den Vorgaben von Art. 5 Abs. 3 der ePrivacy-Richtlinie. Danach wäre zukünftig nur noch das Setzen von notwendigen Cookies ohne Einwilligung der Nutzer erlaubt. Für die Reichweitenmessung, wie sie im öffentlich-rechtlichen Rundfunk zum Zwecke einer bedarfsgerechten Gestaltung seiner Telemedienangebote praktiziert wird, sieht der Entwurf keine ausdrücklichen Erlaubnistatbestände vor. Insofern weicht der Entwurf stark von den bisherigen Regelungen im TMG und auch von dem aktuellen Entwurf der ePrivacy-Verordnung ab, die die ePrivacy-Richtlinie in absehbarer Zeit ablösen wird (s. dazu I. 1.2.).

In der dem Beschluss der Bundesregierung vorausgegangenen Anhörung zum Referentenentwurf hatte auch die RDSK Stellung genommen. Wir hatten um eine Klarstellung dahin gehend gebeten, dass die spezifischen Regelungen der datenschutzrechtlichen Aufsicht im Bereich der Telekommunikation und Telemedien im öffentlich-rechtlichen Rundfunk aufgrund verfassungsrechtlicher Vorgaben unangetastet bleiben. Dies erschien uns erforderlich, um etwaigen Missverständnissen bei der Auslegung der in dem Gesetzentwurf dem BfDI eingeräumten weitreichenden Aufsichtskompetenzen entgegenzuwirken.

Auch die Juristische Kommission von ARD, ZDF und DLR (JuKo) hatte sich in dem Anhörungsverfahren geäußert. Neben der Bitte um Klarstellung im Bereich der Kontrollzuständigkeit hat die Juko vorgeschlagen, die Begründung zum TTDSG dahingehend zu ergänzen, dass die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, zu nicht kommerziellen journalistischen Zwecken keiner Einwilligung bedürfe.

Die Vorschläge von RDSK und Juko haben in dem von der Bundesregierung beschlossenen Entwurf keinen Niederschlag gefunden. Der Bundestag hat den Regierungsentwurf am

25.3.2021 beraten und ihn zur Beratung in die Ausschüsse überwiesen. Parallel dazu wurde der als eilig gekennzeichnete Entwurf am 26.3.2021 im Bundesrat behandelt. Dieser hat in seiner anschließenden Stellungnahme zahlreiche Änderungsvorschläge gemacht, die auch die Wahrung der spezifischen Datenschutzaufsicht über Rundfunk- und Presseunternehmen und des Medienprivilegs im Bereich der journalistisch-redaktionellen Datenverarbeitung betreffen. Der Fortgang des Gesetzgebungsverfahrens bleibt abzuwarten.

1.3. Entwurf eines Telekommunikationsmodernisierungsgesetzes

Am 16.12.2020 hat die Bundesregierung den Entwurf für ein Telekommunikationsmodernisierungsgesetz verabschiedet. Der Bundestag hat dieses Gesetz, mit dem das TKG als Ganzes reformiert werden soll, am 22.4.2021 beschlossen. Nun muss es noch den Bundesrat passieren. Mit dieser umfassenden Novelle soll ein Ordnungsrahmen geschaffen werden, der wichtige Impulse für einen schnelleren und flächendeckenden Ausbau von Gigabitnetzen setzt. Hintergrund der angestrebten Gesetzesänderung ist aber auch die Tatsache, dass Deutschland aktuell ein Vertragsverletzungsverfahren droht, da es der Pflicht zur Umsetzung des europäischen Kodex für die elektronische Kommunikation bis zum 21.12.2020 bisher nicht nachgekommen ist. Diese europäische Richtlinie erfordert eine umfassende Neuregelung des TKG. Danach ist der Begriff des Telekommunikationsdienstes weiter zu fassen. Unter diesen Begriff fallen künftig nicht nur die klassischen Anwendungen wie Telefonie oder SMS, sondern auch internetbasierte Kommunikationsdienste, auch Over-The-Top-Dienste (OTT-Dienste) genannt. Gemeint sind u. a. Messenger, E-Mail und Voice-Over-IP. Die Einbeziehung der OTT-Dienste in die Telekommunikationsregulierung soll in differenzierter Weise erfolgen, d. h. angepasst an deren technische und ökonomische Besonderheiten. Damit sollen chancengleiche Wettbewerbsbedingungen zwischen OTT- und klassischen Telekommunikationsdiensten geschaffen, sowie vergleichbare Standards beispielsweise in den Bereichen Verbraucherschutz und Datenschutz eingeführt werden. So werden sich die im TTDSG vorgesehenen Regelungen zum Fernmeldegeheimnis und Datenschutz auch auf die OTT-Dienste beziehen (s. dazu 1.2.). Die Verpflichtung zur Vorratsdatenspeicherung findet sich nahezu unverändert im Entwurf des Telekommunikationsmodernisierungsgesetzes, obwohl sie per Gerichtsentscheidung aktuell

ausgesetzt ist und nach den Entscheidungen des EuGH vor Gericht kaum Bestand haben dürfte (s. I. 2.2.).

1.4. Gesetz zur Änderung des BND-Gesetzes

Am 16.12.2020 hat das Bundeskabinett einen Entwurf zur Änderung des Gesetzes über den Bundesnachrichtendienst (BND) beschlossen. Die Novelle sieht eine Neuregelung beim technischen Ausspähen von Ausländern außerhalb Deutschlands vor. Nach Befassung von Bundestag und Bundesrat ist das Gesetz nach Ausfertigung durch den Bundespräsidenten inzwischen im Bundesgesetzblatt veröffentlicht worden. Einzelne Teile des Gesetzes (dies gilt insbesondere für die Einrichtung des neu einzurichtenden Kontrollrats) sind seit 22. April 2021 in Kraft. Die weiteren Teile des Gesetzes treten am 1.1.2022 in Kraft.

Hintergrund der Gesetzesänderung ist die Entscheidung des BVerfG zur strategischen Fernmeldeaufklärung im Ausland durch den BND vom 19.5.2020 (1 BvR 2835/17). Als zentrale Frage hatte das BVerfG zu klären, ob der BND im Ausland überhaupt an die Grundrechte gebunden ist. Diese Grundrechtsbindung deutscher Staatsorgane im Ausland hat das BVerfG in dem Urteil zum ersten Mal ausdrücklich bejaht.

Das BND-Gesetz a. F. trug laut BVerfG einer weltweiten Grundrechtsbindung nicht genügend Rechnung. Die Erhebung personenbezogener Daten im Wege der heimlichen Telekommunikationsüberwachung tangierte sowohl den Schutzbereich des durch Art. 10 Abs. 1 GG geschützten Telekommunikationsgeheimnisses als auch den Schutzbereich der in Art. 5 I 2 GG geregelten Pressefreiheit für die als Journalist:innen tätigen Beschwerdeführer. Zwar sei die Befugnis zur Datenerhebung und Datenverarbeitung in Form der Telekommunikationsüberwachung als besonderes Instrument der Auslandsaufklärung grundsätzlich mit Art. 10 Abs. 1 GG und Art. 5 Abs. 1 Satz 2 GG vereinbar, es bedürfe hierfür jedoch einer hinreichend begrenzenden und verhältnismäßigen Ausgestaltung.

Die Novelle sieht eine Vielzahl an Neuregelungen beim technischen Ausspähen von Ausländern außerhalb Deutschlands vor. Zentrale Bestandteile sind die Präzisierung des Erhebungs-

und Verarbeitungsgegenstandes, Einschränkungen des Datenvolumens, die Neufassung der Vorgaben zum Überwachungszweck, Schaffung einer klarer umrissenen Ermächtigungsgrundlage zur Erfassung von Verkehrsdaten, Einfügung von Schutzvorschriften zugunsten besonderer Vertraulichkeitsbeziehungen, die Etablierung von Löschungs- und Protokollpflichten sowie die Schaffung eines unabhängigen Kontrollrates. Der besonderen Schutzstellung von Journalist:innen und anderen Berufen mit besonders vertraulichem Berufsinhalt soll der neu geschaffene § 21 BND-Gesetz gerecht werden, der ausdrücklich bestimmt, dass die Verwendung von Suchbegriffen zur gezielten Erhebung personenbezogener Daten von Rechtsanwält:innen und Journalist:innen sowie Geistlichen zum Zweck der Erlangung von Kenntnissen, die dem Zeugnisverweigerungsrecht unterfallen, unzulässig ist.

Aus Sicht der Medienvertreter bleibt das Gesetz hinter den Erwartungen zurück. Hauptkritik: § 21 bezieht sich ausdrücklich nur auf personenbezogene Daten. Für die sonstige, nicht personenbezogene Aufklärung gibt es in Bezug auf die Berufe mit vertraulichem Berufsinhalt keine Einschränkungen. So unterliegen die sogenannten Verkehrs- bzw. Metadaten keinem Schutz. Ferner wird bemängelt, dass § 21 ausdrücklich nur vor gezielter Kommunikationsüberwachung schützt, so dass sich die Frage stellt, wie mit der ungezielten Datenerfassung mit Blick auf Journalist:innen umgegangen wird. Die aufgezeigten Schwächen dürften Raum für weitere Verfassungsbeschwerden bieten.

1.5. Entwurf eines „Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0)“

Am 16.12.2020 hat das Bundeskabinett auch den Entwurf eines „Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0)“ beschlossen. Der Entwurf ist in Form eines Artikelgesetzes verabschiedet worden, in dem vor allem eine Änderung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-G) vorgesehen ist. Die geplanten Änderungen im BSI-G betreffen im Wesentlichen die Stärkung der Rolle des BSI durch die Zuteilung neuer Aufgaben und Befugnisse. Daneben wurden neue Pflichten für KRITIS (= kritische Infrastrukturen)-Betreiber sowie für die neu eingeführten sogenannten

„Unternehmen von besonderem öffentlichen Interesse“ statuiert. Die Pflicht von KRITIS-Betreibern, angemessene organisatorische und technische Vorkehrungen zu treffen, wurde um die Vorhaltung von Systemen zur Angriffserkennung ergänzt, um Cyberangriffen effektiv begegnen und den Schaden reduzieren zu können.

Das BSI-G regelt den Sektor ‚Medien und Kultur‘ schon deshalb nicht, weil dieser Ländersache ist. Dies soll nach dem vorliegenden Entwurf auch nicht geändert werden. Die Rundfunkanstalten haben im Rahmen ihrer Anhörung dennoch angeregt, entsprechende Klarstellungen in das Gesetz aufzunehmen.

Die öffentlich-rechtlichen Rundfunkanstalten betrachten die Gewährleistung der IT-Sicherheit für die von ihnen betriebenen Intrastrukturen als Teil ihrer gesetzlichen Aufgaben. Aus diesem Grund engagieren sie sich im Branchenarbeitskreis Medien des UP KRITIS (=öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen in Deutschland). Die Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik BSI und weiteren Akteuren im Bereich Cybersicherheit Deutschlands hatte für ARD; ZDF und Deutschlandradio schon immer einen großen Stellenwert. Allerdings muss der Gesetzgeber darauf achten, dass erweiterte staatliche Befugnisse und Verpflichtungen der verschiedenen Marktteilnehmer die verfassungsrechtlich erforderlichen Grenzen zur Wahrung der Rundfunk- und Pressefreiheit einhalten. Alle staatlichen Eingriffe – zu denen auch die polizeilichen und aufsichtsrechtlichen Befugnisse des BSI und anderer Behörden gehören – müssen zwingend Ausnahmetatbestände für den journalistischen Bereich vorsehen.

2. Entscheidungen

2.1. BGH-Entscheidungen zum Recht auf Vergessenwerden

Der Bundesgerichtshof (BGH) hat sich in zwei Verfahren vom 27.7.2020 gegen den Suchmaschinenbetreiber Google zu dem sogenannten „Recht auf Vergessenwerden“ (Art. 17 DSGVO) geäußert.

Im Verfahren VI ZR 405/18 ist er der Rechtsprechung des EuGH und des BVerfG gefolgt und hat in seiner Entscheidung klargestellt, dass ein Auslistungsanspruch gegen einen US-amerikanischen Suchmaschinenbetreiber grundsätzlich auf Art. 17 DSGVO gestützt werden kann. Die Tätigkeit eines Suchmaschinenbetreibers, die darin besteht, von Dritten ins Internet gestellte und dort veröffentlichte Informationen zu finden, automatisch zu indexieren, vorübergehend zu speichern und schließlich den Internet-Nutzern in einer bestimmten Rangfolge zur Verfügung zu stellen, falle, sofern die Informationen personenbezogene Daten enthalten, in den sachlichen Anwendungsbereich der DSGVO. Diese Tätigkeit unterliege auch nicht dem Medienprivileg, da die automatisierte bloße Auflistung von redaktionellen Beiträgen keine eigene journalistisch-redaktionelle Gestaltung darstelle. Der räumliche Anwendungsbereich der DSGVO auf den in den USA ansässigen Suchmaschinenbetreiber folge aus der Tatsache, dass er eine deutsche Niederlassung betreibe und in deutscher Sprache Nutzer:innen in Deutschland die Möglichkeit anbiete, über ihren Suchdienst gezielt nach im Internet vorhandenen Informationen zu suchen (Art. 3 Abs. 1 DSGVO).

Der Auslistungsanspruch erfordere eine Grundrechtsabwägung der Grundrechte des Klägers auf der einen und des Suchmaschinenbetreibers auf der anderen Seite. In die Abwägung sei zudem auch das Grundrecht der Inhalteanbieter auf freie Meinungsäußerung gemäß Art. 11 GRCh einzubeziehen. Außerdem seien die Zugangsinteressen der Internetnutzer in die Abwägung einzustellen. Zu berücksichtigen sei das Interesse einer breiten Öffentlichkeit am Zugang zu Information. Es gelte keine Vermutung eines Vorrangs der Schutzinteressen des Betroffenen. Vielmehr seien die sich gegenüberstehenden Grundrechte gleichberechtigt miteinander abzuwägen. Aus diesem Gebot folge aber auch, dass der Verantwortliche einer Suchmaschine nicht erst dann tätig werden muss, wenn er von einer offensichtlichen und auf den ersten Blick klar erkennbaren Rechtsverletzung des Betroffenen Kenntnis erlangt.

Diese neue Rechtsprechung des BGH stärkt das Recht auf Vergessenwerden der Betroffenen. Durch die Pflicht zur Einzelfallabwägung und der Gleichstellung der Interessen der Inhalteanbieter scheidet allerdings die grundsätzliche Vermutung des Vorrangs der

Schutzinteressen der Betroffenen aus. Dadurch wird zugleich die Meinungs- und Pressefreiheit gestärkt, da sich ein pauschales und schemenhaftes Ergebnis verbietet.

In dem Verfahren mit dem Aktenzeichen VI ZR 476/18 begehrten die Kläger von dem Verantwortlichen für die Internetsuchmaschine Google, es zu unterlassen, bestimmte Artikel bei der Suche nach ihren Namen in der Ergebnisliste nachzuweisen und Fotos von ihnen anzuzeigen. Der für Google Verantwortliche hatte erklärt, die Wahrheit der in den verlinkten Inhalten aufgestellten Behauptungen nicht beurteilen zu können. Die Klage blieb in beiden Vorinstanzen erfolglos. Das Berufungsgericht hat angenommen, dass die von der Beklagten vorgenommene Verarbeitung der personenbezogenen Daten der Kläger rechtmäßig erfolgt sei und sich ein Auslistungsanspruch daher nicht auf Art. 17 DSGVO stützen lasse. Die Kläger hätten die Wahrheitswidrigkeit der über sie berichteten Tatsachen nicht belegen können. Auch hinsichtlich der angezeigten Fotos sei eine offensichtliche und für den Suchmaschinenbetreiber auf der Hand liegende Rechtsverletzung nicht ersichtlich, da die Bilder im Hinblick auf die veröffentlichten Artikel Bildnisse aus dem Bereich des Zeitgeschehens sein könnten.

Der BGH hat das Verfahren ausgesetzt und dem EuGH zwei Fragen zur Vorabentscheidung vorgelegt. Die erste Frage behandelt den Auslistungsantrags eines Links, der zu einem Beitrag führt, deren Wahrheit der Betroffene verneint. Der BGH möchte wissen, ob es zulässig ist, bei der Abwägung der widerstreitenden Interessen auch darauf abzustellen, ob der Betroffene in zumutbarer Weise „Vorarbeit“ in Form der Nachweiserbringung des Wahrheitsgehalts erbringen könnte. Dies könnte der Betroffene leisten, indem er Rechtsmittel gegen den Inhalteanbieter einlegt. So wäre die Frage der Wahrheit des Inhaltes vorab geklärt, was sich wiederum auf das Auslistungsbegehren auswirken würde.

Die zweite Frage des BGH betrifft den Fall eines Auslistungsbegehrens gegen den Verantwortlichen eines Internet-Suchdienstes, der bei einer Namenssuche nach Fotos von natürlichen Personen sucht, die Dritte im Zusammenhang mit dem Namen der Person ins Internet eingestellt haben, und der die von ihm aufgefundenen Fotos in seiner Ergebnisübersicht als Vorschaubilder (‚thumbnails‘) zeigt. Der BGH will wissen, ob im Rahmen der

vorzunehmenden Abwägung der widerstreitenden Rechte und Interessen der Kontext der ursprünglichen Veröffentlichung des Dritten maßgeblich zu berücksichtigen ist, auch wenn die Webseite des Dritten bei Anzeige des Vorschaubildes durch die Suchmaschine zwar verlinkt, aber nicht konkret benannt und der sich hieraus ergebende Kontext vom Internet-Suchdienst nicht mit angezeigt wird. Eine aktuelle Entscheidung des EuGH mit Blick auf die Vorlagen des BGH steht aktuell noch aus.

2.2. Urteil des BGH zur wirksamen Erteilung einer Einwilligung für Cookies

In seinem Urteil vom 28.5.2020 (I ZR 7 /16) hat sich der BGH erneut mit den Anforderungen an die Einwilligung hinsichtlich der Speicherung von Cookies auf dem Endgerät eines Nutzers auseinandergesetzt. Mit Beschluss vom 5.10.2017 hatte er das Verfahren zunächst ausgesetzt und dem EuGH verschiedene Fragen zur Auslegung des Unionsrechts in Bezug auf die Wirksamkeit einer Einwilligung in das Setzen von Cookies durch ein voreingestelltes Ankreuzkästchen vorgelegt. Hierzu hat der EuGH mit Urteil vom 1.10.2019 (C-673/17) die vorgelegten Fragen beantwortet und die Anforderungen an eine wirksame Einwilligung in die Speicherung von Cookies oder den Zugriff auf Informationen, die bereits im Endgerät der Nutzer einer Website gespeichert sind, konkretisiert (s. dazu auch 16. Tätigkeitsbericht, S. 17 f.). Danach ist unter Berücksichtigung der einschlägigen europäischen Richtlinien ein voreingestelltes Ankreuzkästchen, das der Nutzer zur Verweigerung seiner Einwilligung abwählen muss, nicht ausreichend. Vielmehr muss dem Setzen der Cookies aktiv zugestimmt werden.

Im Revisionsverfahren hat der BGH nun auf Grundlage der bindenden Vorgaben des EuGH-Urteils entschieden, dass die Einwilligung in das Setzen von Cookies mittels eines bereits voreingestellten Ankreuzkästchens eine unangemessene Benachteiligung der Nutzer darstelle und damit unwirksam sei. Eine derartige Einwilligung sei mit dem wesentlichen Grundgedanken des § 15 Abs. 3 Satz 1 TMG nicht vereinbar. Diese Vorschrift erlaube zwar die Erstellung von Nutzungsprofilen zum Zwecke der Werbung unter der Verwendung von Pseudonymen, sofern die Nutzer dem nicht widersprechen (sog. Opt-Out). Im Hinblick auf die Entscheidung des EuGH sei § 15 Abs. 3 Satz 1 TMG jedoch dahingehend auszulegen, dass für den Einsatz von

nicht notwendigen Cookies stets die Einwilligung der Nutzer erforderlich sei. Die Einwilligung müsse dabei ausdrücklich im Wege eines aktiven Setzens des Ankreuzhäkchens erklärt werden (sog. Opt-In). Diese Auslegung sei mit dem Wortlaut des § 15 Abs. 3 Satz 1 TMG vereinbar.

Die Praxis der öffentlich-rechtlichen Rundfunkanstalten beim Setzen von Cookies zur Reichweitenmessung ist von der Rechtsprechung des BGH nach Auffassung der RDSK nicht tangiert. § 15 Abs. 3 TMG sollte es den Telemedienanbietern ursprünglich ermöglichen, auch ohne Einwilligung pseudonymisierte Nutzungsprofile „für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung ihrer Telemedien“ anzulegen. Nach ihrem Sinn und Zweck zielte die Vorschrift darauf, dem Verantwortlichen das Anlegen personalisierter Nutzerprofile für die genannten Zwecke zu erleichtern. Eine anonymisierte Nutzungsmessung ermöglicht den Rundfunkanstalten jedoch keine personalisierbare, sondern eine auf ihr Onlineangebot insgesamt bezogene statistische Auswertung. Daher unterfällt die Nutzungsmessung der Rundfunkanstalten dem Anwendungsbereich des § 15 Abs.3 TMG und dem nach Auffassung des BGH dort postulierten Einwilligungserfordernis nicht (s. dazu auch die „Empfehlungen der RDSK zum Einsatz von Cookies in Online-Angeboten der Rundfunkanstalten“ mit Stand September 2020; Anlage 2).

III. Berlin/Brandenburg

1. Gesetze

1.1. Berliner Datenschutz-Anpassungsgesetz EU

Am 25.10.2020 ist das Berliner Datenschutz-Anpassungsgesetz EU in Kraft getreten. Während mit der Neufassung des Berliner Datenschutzgesetzes (BlnDSG) vom 13. Juni 2018 der sich aus der DSGVO ergebende Anpassungsbedarf im allgemeinen Datenschutzrecht auf Landesebene bereits umgesetzt worden ist, fehlte bislang die Anpassung der bereichsspezifischen Landesgesetze an die DSGVO. Diese Anpassung ist Gegenstand des Berliner Datenschutz-Anpassungsgesetzes EU. Nunmehr sind auch die Spezialgesetze wie das Landeswahlgesetz, das Berliner Informationsfreiheitsgesetz, die Bauordnung von Berlin etc. an die unionsrechtlichen Vorgaben angepasst. Auch das BlnDSG ist an einigen wenigen Stellen erneut geändert worden.

Für den rbb allein relevant ist die Entscheidung, dass § 3 BlnDSG als nachrangige Auffangregelung für die Verarbeitung von personenbezogenen Daten mit geringer Eingriffsintensität in die Rechte der betroffenen Personen dauerhaft weiter gilt. Die Schaffung einer solchen Rechtsgrundlage ist grundsätzlich erforderlich, da Art. 6 Abs. 3 Satz 1 DSGVO für die Verarbeitung personenbezogener Daten im öffentlichen Interesse eine Rechtsgrundlage verlangt, die durch Unionsrecht oder das Recht eines Mitgliedsstaates festgelegt wird. Art. 6 Abs. 1 c) und e) DSGVO stellen selbst keine Rechtsgrundlagen für die Verarbeitung personenbezogener Daten dar, sondern setzen sie voraus.

1.2. 23. Rundfunkänderungsstaatsvertrag

Am 1.6.2020 ist der 23. Rundfunkänderungsstaatsvertrag (RÄndStV) in Kraft getreten. Schwerpunkte sind in Art. 1 (Änderung des Rundfunkbeitragsstaatsvertrages/RBStV) die Umsetzung der Vorgaben des BVerfG zur Befreiung von der Rundfunkbeitragspflicht für Zweitwohnungsinhaber:innen und die Einführung eines regelmäßigen, alle vier Jahre stattfindenden, Meldedatenabgleichs – beginnend ab dem Jahr 2022. Zur Wahrung der Verhältnismäßigkeit zwischen Beitragsgerechtigkeit und dem Schutz persönlicher Daten erfolgt der Meldeabgleich nicht, wenn die Kommission zur Ermittlung des Finanzbedarfs der Rundfunkanstalten (KEF) in ihrem Bericht nach § 3 Abs. 8 des Rundfunkfinanzierungsstaatsvertrages feststellt, dass der Datenbestand hinreichend aktuell ist (§ 11 Abs. 5 Satz 5 RBStV). Mit dem regelmäßigen Meldedatenabgleich soll die Verhältnismäßigkeit zwischen Beitragsgerechtigkeit und dem Recht auf informationelle Selbstbestimmung gewahrt werden. Die weiteren Anpassungen im 23. RÄndStV sind Folgeänderungen aufgrund der DSGVO. Unter anderem ist der Umfang des datenschutzrechtlichen Auskunftsanspruchs konkretisiert worden.

Nach Auffassung des Arbeitskreises der Datenschutzbeauftragten des öffentlich-rechtlichen Rundfunks (AK DSB) handelt es sich bei dem regelmäßigen Meldedatenabgleich um eine verhältnismäßige Maßnahme, die der Vermeidung eines Vollzugsdefizits und der Herstellung größerer Beitragsgerechtigkeit dient. Die einschränkende Regelung des datenschutzrechtlichen

Auskunftsanspruchs trägt dem Massenverfahren beim Zentralen Beitragsservice (ZBS) Rechnung und wird den Anforderungen des Art. 23 DSGVO gerecht.

1.3. Staatsvertrag zur Modernisierung der Medienordnung in Deutschland

Am 7.11.2020 ist der Staatsvertrag zur Modernisierung der Medienordnung in Deutschland in Kraft getreten. Wichtigster Bestandteil ist der neue Medienstaatsvertrag (MStV). Dieser hat den Rundfunkstaatsvertrag (RStV) abgelöst, der seit 1991 galt und immer wieder geändert und ergänzt worden war (s. dazu auch 1.2.). Die Umbenennung soll deutlich machen, dass das Gesetz jetzt nicht mehr nur für Fernsehen und Radio, sondern auch für die vielen anderen ausschließlich digitalen Medienangebote gilt. Das betrifft u. a. die Medienintermediäre, also Vermittler zwischen Medieninhalten wie Facebook oder Google, aber auch Smart-TV, Voice-Assistenten, Videostreamer und Blogs. Wer wie Google oder Facebook Medieninhalte verbreitet, ist nun zur Transparenz verpflichtet. Die Anbieter müssen etwa erklären, nach welchen Kriterien sie Inhalte gewichten und anzeigen. Außerdem dürfen journalistisch-redaktionelle Angebote nicht gegenüber jeweiligen Konkurrenzangeboten diskriminiert werden. Die Regelungen zum datenschutzrechtlichen Medienprivileg finden sich unverändert in § 12 bzw. für Telemedien in § 23 MStV (bisher § 9 c bzw. § 57 RStV).

1.4. Erster Medienänderungsstaatsvertrag

In der Zeit vom 10. bis 17.6.2020 haben die Regierungschef:innen der Länder den Ersten Medienänderungsstaatsvertrag (MÄndStV) unterzeichnet. Inhalt ist zum einen die Umsetzung der von der KEF in ihrem 22. Bericht ausgesprochenen Empfehlung für eine Erhöhung des Rundfunkbeitrags in der nächsten Beitragsperiode (Zeitraum 2021 bis 2024). Vorgesehen war eine Anhebung des monatliche Rundfunkbeitrags um 86 Cent von derzeit 17,50 EUR auf 18,36 EUR ab dem 1.1.2021. Zum anderen sieht der Staatsvertrag eine Anpassung des zugunsten von Radio Bremen (RB) und des Saarländischen Rundfunks (SR) bestehenden ARD-Finanzausgleichs durch eine schrittweise Anhebung der Finanzausgleichsmasse vor. Alle Länderparlamente bis auf Sachsen-Anhalt haben dem Ersten MÄndStV zugestimmt. Ministerpräsident

Haseloff hat die Vorlage zum Gesetz zur Ratifizierung in Sachsen-Anhalt aus politischen Gründen zurückgezogen. Damit ist es nicht zur Abstimmung im Landtag von Sachsen-Anhalt gekommen, sodass der Staatsvertrag nicht zum 1.1.2021 in Kraft treten konnte. Gegen diese Entscheidung haben die Landesrundfunkanstalten der ARD, das ZDF und DLR gemeinsam das Bundesverfassungsgericht angerufen. Sie haben eine einstweilige Anordnung beantragt (Eilverfahren) und gleichzeitig Verfassungsbeschwerde eingelegt. Das BVerfG hat den Eilantrag am 22.12.2020 zurückgewiesen. Zur Begründung führte das Gericht an, dass die Rundfunkanstalten nicht in der den gesetzlichen Anforderungen an die Begründung gemäß § 23 Abs. 1 Satz 2, § 92 BVerfG-Gesetz entsprechenden Weise dargelegt hätten, dass ihnen durch ein Abwarten bis zum Abschluss des Verfassungsbeschwerdeverfahrens schwere Nachteile im Sinne des § 32 Abs. 1 BVerfG-Gesetz entstehen. Das Verfassungsbeschwerdeverfahren dauert weiter an.

2. Entscheidungen

2.1. Urteil des LAG Berlin-Brandenburg zur Zulässigkeit eines biometrischen Zeiterfassungssystems

Am 4.6.2020 hat das Landesarbeitsgericht (LAG) Berlin-Brandenburg ein Urteil zur Zulässigkeit der Verwendung von biometrischen Zeiterfassungssystemen erlassen (10 Sa 2130/19).

Geklagt hatte ein Arbeitnehmer auf Entfernung von Abmahnungen aus seiner Personalakte. Den Abmahnungen lag folgender Sachverhalt zugrunde: Der Arbeitgeber hatte im August 2018 ein neues Zeiterfassungssystem eingeführt, bei dem sich die Mitarbeiter:innen mit ihrem Fingerabdruck an- und abmelden mussten. Dabei erfolgte ein Abgleich des Fingerabdrucks mit zuvor im Zeiterfassungsterminal gespeicherten Daten. Hierfür wurden aus dem Fingerabdruck des Mitarbeiters sogenannte Minutien, also individuelle Fingerlinienverzweigungen, mit einem speziellen Algorithmus extrahiert und im Zeiterfassungsterminal gespeichert. Der Arbeitnehmer hatte sich geweigert, das Zeiterfassungssystem zu nutzen. Aus diesem Grund erteilte der Arbeitgeber ihm insgesamt zwei Abmahnungen. Nach Auffassung des Arbeitgebers ist die

Verarbeitung der biometrischen Daten im Rahmen der Zeiterfassung erforderlich. Alle anderen Zeiterfassungssysteme seien manipulierbar. Zudem würde kein kompletter Fingerabdruck genommen, sondern nur die Minutien erfasst.

Die Klage des Arbeitnehmers auf Entfernung seiner Abmahnungen aus der Personalakte hatte vor dem Arbeitsgericht Berlin Erfolg und wurde durch das Urteil des LAG Berlin-Brandenburg bestätigt.

Das LAG stellte zunächst fest, dass es sich bei dem verwendeten Minutiendatensatz um biometrische Daten im Sinne von Art. 9 Abs. 1 DSGVO sowie um personenbezogene Daten nach § 26 Abs. 3 BDSG handelt, auch wenn nicht der komplette Fingerabdruck verarbeitet wird.

Eine Verarbeitung der biometrischen Daten ist grundsätzlich verboten. Sie ist nur in Ausnahmefällen möglich, wenn entweder eine freiwillige Einwilligung des Arbeitnehmers vorliegt oder aber die Verarbeitung der Daten erforderlich ist, soweit dies nach Unionsrecht oder dem Recht der Mitgliedsstaaten oder einer Kollektivvereinbarung zulässig ist. Da weder eine Einwilligung noch eine Kollektivvereinbarung vorlagen, prüften die Richter, ob die Datenverarbeitung nach § 26 Abs. 3 BDSG erforderlich war. Der Arbeitgeber darf danach personenbezogene Daten verarbeiten, wenn dies für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist. Dies verneinten die Gerichte.

In der Urteilsbegründung wiesen die Richter darauf hin, dass die Grundrechte und Grundfreiheiten der betroffenen Personen durch die Verwendung der biometrischen Daten erheblich beeinträchtigt würden. Die Tatsache, dass vereinzelt ein Missbrauch von Zeiterfassungssystemen durch Falscheintragungen oder im Falle einer Stempelkarte durch ‚mitstempeln' durch Kolleg:innen auftreten könne, mache eine Kontrolle per Fingerprint nicht nötig. Grundsätzlich sei davon auszugehen, dass die überwiegende Mehrheit der Beschäftigten sich rechtstreu verhalte. Nur bei konkreten Nachweisen über erhebliche Missbräuche könne eine solche Maßnahme aus Sicht des Gerichts erforderlich sein.

Biometrische Merkmale werden im Arbeitsleben in vielen Fällen erfasst und verarbeitet. Dies gilt z. B. für die Identitätsfeststellung bei der Zeiterfassung, beim Einsatz von

Zahlungssystemen, bei der Zugangsberechtigung oder der Zugriffs-Authentisierung zu IT-Systemen. Die Entscheidung der Berliner Gerichte macht jedoch deutlich, dass bei der Verarbeitung von Daten im Sinne des Art. 9 Abs. 1 DSGVO ein erhöhter Erforderlichkeitsnachweis vonnöten ist, der hinreichend belegt werden muss. Eine Maßnahme, die für „bequemer" gehalten wird, erfüllt nicht den Maßstab der hinreichend darzulegenden Erforderlichkeit. Der rbb hat bislang auf die Nutzung von biometrischen Merkmalen seiner Beschäftigten verzichtet.

2.2. Beschluss des LG Berlin zur Einstellung des Ordnungswidrigkeitsverfahren gegen die Deutsche Wohnen SE

Wie berichtet (16. Tätigkeitsbericht S. 36 ff.), hat die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) im Herbst 2019 einen Bußgeldbescheid über 14,5 Millionen Euro gegen eines der größten deutschen Immobilienunternehmen Deutschlands, die Deutsche Wohnen SE, erlassen. Die Deutsche Wohnen SE hatte es über Jahre unterlassen, veraltete Daten der Mieter:innen zu löschen. Dagegen hatte die Deutsche Wohnen SE Einspruch eingelegt. Mit Beschluss vom 18.2.2021 hat das Landgericht (LG) Berlin festgestellt, dass der Bußgeldbescheid aufgrund gravierender Mängel nicht Grundlage des Verfahrens sein könne. Der Bescheid enthalte keine Angaben zu konkreten Tathandlungen eines Organs des Unternehmens und sei deshalb unwirksam. Nach deutschem Recht könne nur eine natürliche Person vorwerfbar eine Ordnungswidrigkeit begehen. Der juristischen Person könne lediglich ein Handeln ihrer Organmitglieder oder Repräsentant:innen zugerechnet werden. Mit dieser Begründung hat das LG das Verfahren eingestellt.

Ob die Voraussetzungen des deutschen Ordnungswidrigkeitenrechts auch für die Festsetzung von Bußgeldern nach der DSGVO gelten, ist umstritten. Nach anderer Ansicht geht das Unionsrecht von der sogenannten unmittelbaren Verbandshaftung aus, bei der Geldbußen gegen Unternehmen und nicht gegen einzelne Rechtsträger:innen verhängt werden, mit der Folge, dass das Bußgeld und der zu Grunde liegende Verstoß unmittelbar an das Unternehmen geknüpft werden kann. So hat beispielsweise das LG Bonn in einem Urteil vom 11.11.2020 die Verhängung eines Bußgeldes gegen ein Tochterunternehmen eines der größten

Telekommunikationsdienstleister in Deutschland für rechtens erkannt. Auch in diesem Fall hatte der den Bußgeldbescheid erlassende BfDI nicht näher beschrieben, welche natürlichen Personen im Unternehmen durch welche Handlungen den Datenschutzverstoß begangen haben. Die Staatsanwaltschaft Berlin hat auf Betreiben der BlnBDI Beschwerde gegen den Beschluss eingelegt.

Da gegen den rbb als öffentliche Stelle i. S. v. § 2 BlnDSG generell keine Geldbußen verhängt werden können, ist er von dieser Rechtsprechung nicht unmittelbar tangiert. In besonders gelagerten Ausnahmefällen könnten im Fall von grob fahrlässigen oder vorsätzlichen Datenschutzverstößen jedoch Geldbußen gegenüber einzelnen Mitarbeiter:innen verhängt werden.

IV. Wichtige Entscheidungen aus anderen Bundesländern

1. Urteil des Oberverwaltungsgerichts Rheinland-Pfalz zur gerichtlichen Kontrolle einer aufsichtsbehördlichen Beschwerdeentscheidung

Mit Urteil vom 26.10.2020 hat das Oberverwaltungsgericht (OVG) Rheinland-Pfalz wichtige Aussagen zum Umfang der gerichtlichen Kontrolle einer aufsichtsbehördlichen Beschwerdeentscheidung nach Art. 78 Abs. 1 DSGVO getroffen, die über Rheinland-Pfalz hinaus Bedeutung für alle Aufsichtsbehörden haben. Danach beschränkt sich die gerichtliche Kontrolle einer aufsichtsbehördlichen Beschwerdeentscheidung nach Art. 78 Abs. 1 DSGVO grundsätzlich darauf, ob die Behörde sich mit der Beschwerde befasst, den Beschwerdegegenstand angemessen untersucht und den Beschwerdeführer über das Ergebnis der Prüfung unterrichtet hat.

Dem Urteil lag folgender Sachverhalt zugrunde: Der Kläger hatte im Oktober 2018 beim Datenschutzbeauftragten der beigeladenen Stadt geltend gemacht, personenbezogene Daten zu seiner Person seien ohne seine Zustimmung vermutlich vom Bürgeramt oder dem Tiefbauamt der Beigeladenen an die Zulassungsstelle weitergegeben worden. Dies stelle einen Verstoß gegen das Datenschutzgesetz dar; er bitte um eine entsprechende Bescheinigung über diesen Datenmissbrauch. Nachdem dieses Schreiben zunächst unbeantwortet geblieben war, hat

sich der Kläger an den Landesbeauftragten für den Datenschutz und für die Informationsfreiheit Rheinland-Pfalz gewandt. Auf dessen Aufforderung hat der Datenschutzbeauftragte der beigeladenen Stadt zu dem vom Kläger vorgetragenen Sachverhalt Stellung genommen und mitgeteilt, der Kläger habe einen Antrag auf Erteilung einer Parkberechtigung bei der Straßenverkehrsbehörde der Beigeladenen gestellt. Auf dem entsprechenden Antragsformular werde darauf hingewiesen, dass die Genehmigungsbehörde die Angaben des Antragstellers überprüfe und sich hierzu die erforderlichen Auskünfte u. a. aus dem Melde- oder Kfz-Zulassungsregister einholen könne. Mit der Unterzeichnung des Antrags habe sich der Kläger damit einverstanden erklärt.

Auf ein weiteres Auskunftsersuchen, ob bzw. welche personenbezogenen Daten die Stadtverwaltung zu seiner Person verarbeitete, hat der Datenschutzbeauftragte der Beigeladen den Kläger zunächst ersucht, sein Auskunftsersuchen zu präzisieren. Da nicht ausgeschlossen werden könne, dass die Stadtverwaltung eine große Menge von Informationen zu seiner Person verarbeite, werde er um Mitteilung gebeten, auf welche Informationen oder welche Verarbeitungsvorgänge sich sein Auskunftsersuchen beziehe. Nachdem der Kläger dieses Schreiben ebenfalls an den beklagten Landesdatenschutzbeauftragten weitergeleitet hatte, teilte dieser dem Kläger im Wege einer Zwischennachricht mit, dass die Stadt zu dem vom Kläger vorgetragenen Sachverhalt Stellung genommen habe. Angesichts des Hinweises auf dem vom Kläger unterzeichneten Antragsformular sei die Datenverarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe der Stadt erforderlich und zulässig. Die Bitte der Stadt um Präzisierung des ebenfalls geltend gemachten Auskunftsrechts nach Art. 15 DSGVO sei im Hinblick auf die Vielzahl von Verarbeitungstätigkeiten gemäß Erwägungsgrund 63 DSGVO berechtigt. Einige Zeit später teilte der Landesdatenschutzbeauftragte dem Kläger unter Beifügung einer Rechtsmittelbelehrung mit, dass ein Datenschutzverstoß nicht vorliege. Da der Kläger keine neuen Aspekte vorgetragen habe, die eine andere Wertung nahelegten, werde das Verfahren beendet.

Gegen diese Entscheidung hat der Kläger Klage vor dem VG Koblenz erhoben und zur Begründung vorgetragen, dass diese Entscheidung inhaltlich falsch sei. Das VG Koblenz hat die Klage mit Urteil vom 16.3.2020 mit der Begründung abgewiesen, der beklagte

Landesdatenschutzbeauftragte habe die Beschwerde des Klägers in angemessener Weise geprüft und den Kläger hinreichend über seine datenschutzrechtliche Einschätzung unterrichtet. Der Datenabgleich sei rechtmäßig gewesen. Auch die Bitte der Stadt um Mitteilung, auf welche Datenverarbeitungsvorgänge sich sein Auskunftsersuchen richte, verletze seine Rechte aus der DSGVO nicht. Zum einen habe der Kläger gegenüber der Aufsichtsbehörde keinen Anspruch auf eine bestimmte Sachentscheidung. Zum anderen sei es von dem weiten Ermessen des Beklagten gedeckt, dass dieser die Aufforderung des Datenschutzbeauftragten zur Präzisierung des Auskunftsersuchens nicht beanstandet habe. Über die dagegen eingelegte Berufung hat das OVG mit Urteil vom 26.10.2020 entschieden. Danach ist die Klage unbegründet. Der Kläger hat keinen Anspruch auf Verpflichtung des Beklagten zur Neubescheidung seiner Beschwerde. Rechtsgrundlage der Beschwerdeentscheidung ist Art. 57 Abs. 1 lit. f) DSGVO. Erhebt eine betroffene Person eine Beschwerde im Sinne von Art. 77 DSGVO, muss sich die Aufsichtsbehörde nach Art. 57 Abs. 1 lit. f) DSGVO mit der Beschwerde befassen, den Gegenstand der Beschwerde in angemessenem Umfang untersuchen und den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung unterrichten. Ergänzend bestimmt Art. 77 Abs. 2 DSGVO, dass die Aufsichtsbehörde den Beschwerdeführer über die Möglichkeit eines gerichtlichen Rechtsbehelfs nach Art. 78 DSGVO unterrichtet; diese Unterrichtung hat gemäß § 78 Abs. 2 DSGVO binnen drei Monaten zu erfolgen. Welcher Untersuchungsumfang bei der Bearbeitung einer Beschwerde als angemessen anzusehen ist, regelt Art. 57 DSGVO nicht. Insoweit folge aus Erwägungsgrund (EG) 141 Satz 2 DSGVO, dass die Untersuchung vorbehaltlich gerichtlicher Überprüfung soweit gehen sollte, wie dies im Einzelfall angemessen sei. Maßstab für den Umfang der Ermittlungen ist danach insbesondere die individuelle Bedeutung der Sache und die Schwere des in Rede stehenden Verstoßes. Die Untersuchung selbst hat nach der Rechtsprechung des EuGH mit aller gebotenen Sorgfalt zu erfolgen. Zu der abschließenden Mitteilung an die betroffene Person gehören die Ergebnisse der tatsächlichen Prüfung sowie deren rechtliche Bewertung. Nach Maßgaben dieser Grundsätze hat der beklagte Landesdatenschutzbeauftragte seine Pflichten bei der Bearbeitung der Beschwerde des Klägers erfüllt.

C. Datenschutz und Datensicherheit im rbb

I. Regelwerke im rbb

1. Allgemeines

Zur Regelung des Umgangs mit IT-Systemen müssen als sogenannte organisatorische Maßnahmen zum Datenschutz Ge- und Verbote für die Beschäftigten festgelegt werden. Um verbindlich zu sein, müssen sie eindeutig formuliert und den Beschäftigten bekannt sein. Aktuell sind diese Anforderungen aus Sicht der Datenschutzbeauftragten im rbb nicht optimal umgesetzt. Neben der Veröffentlichung im rbb-Handbuch finden sich inzwischen an den unterschiedlichsten Stellen im Intranet Hinweise zu IT-Systemen und neuen Verfahren, wobei oftmals für die Beschäftigten nicht klar erkennbar ist, ob es sich nur um Empfehlungen, oder um verbindliche Maßgaben handelt. Diese Unklarheiten können zulasten der Durchsetzbarkeit gehen. Um eine höhere Verbindlichkeit zu erreichen, habe ich mich gemeinsam mit dem Leiter der Revision mit dem Ziel einer Verbesserung des Verfahrens bei der Ausarbeitung und Veröffentlichung von verbindlichen Handlungsanweisungen an die HA Personal gewendet. Die Gespräche sind noch nicht abgeschlossen.

2. Dienstanweisung Informationsmanagement

Wie im letzten Tätigkeitsbericht dargestellt (16. Tätigkeitsbericht, S. 38 ff.), hatte ich gemeinsam mit den Kollegen aus der Informationssicherheit die Dienstanweisung (DA) Informationsmanagement mit elf Anlagen erarbeitet. Darin sind sämtliche Anforderungen an die Verarbeitung von Daten und Informationen im rbb zusammengefasst. Nach Beschlussfassung durch die Geschäftsleitung, Ausfertigung durch die Intendantin und anschließender Veröffentlichung im Intranet ist die DA Informationsmanagement im Juni 2020 in Kraft getreten. Aufgrund des im Vorfeld geführten intensiven Dialogs zu den Inhalten mit den Mitgliedern des IT-Sicherheitskreises, den Datenschutzkoordinator:innen und den Mitarbeitervertretungen waren viele Kolleg:innen von Anfang an damit vertraut. Dies hat die Akzeptanz befördert und den Umsetzungsprozess erleichtert.

Erste Änderungen hat die DA bereits im November 2020 erfahren. Neben kleineren Modifizierungen des Verfahrens zur Beantragung von IT-Nutzerberechtigungen musste Anlage 4 (‚Auftragsverarbeitung') an die Rechtslage nach dem ‚Schrems II'-Urteil des EuGH vom 16.7.2020 angepasst werden (s. B. I. 2.1.). Danach kann eine Neuvergabe von Aufträgen an Anbieter aus den USA nur im Ausnahmefall und mit Zustimmung der Datenschutzbeauftragten erfolgen. Für die Klärung, ob die Beauftragung eines Anbieters aus den USA ausnahmsweise infrage kommt, ist entscheidend, welcher Informationsklasse die zu verarbeitenden personenbezogenen Daten angehören und welche zusätzlich zu der Vereinbarung zur Auftragsverarbeitung und den Standardvertragsklauseln ergriffenen technischen und organisatorischen Maßnahmen geplant sind.

In Anlage 7 der DA ist die Klassifizierung von papiergebundenen und elektronischen Daten und Informationen geregelt. Die Klassifizierung spielt bereits bei der Planung neuer Systeme eine Rolle. Von der Daten- bzw. Informationsklasse leitet sich deren jeweiliger Schutzbedarf ab. Die Klassifizierung orientiert sich an den relevanten Risiken und dem möglichen Schaden, den ein etwaiger Missbrauch verursachen könnte. Je höher der Schutzbedarf ist, desto mehr technischer und organisatorischer Aufwand muss zum Schutz der Daten und Informationen betrieben werden. Bei der Anwendung von IT-Systemen sind alle Beschäftigten aufgefordert, vor der Verarbeitung von Daten eine Klassifizierung vorzunehmen, damit die für die jeweilige Klasse eingerichteten automatischen Schutzmaßnahmen greifen können bzw. – soweit ein automatischer Schutz nicht eingerichtet werden konnte – entsprechende Schutzmaßnahmen wie z. B. Verschlüsselung von den Beschäftigten selbst ergriffen werden.

Die Klassifizierung ist ein wichtiges Instrument zum Schutz von Daten und Informationen und gehört zu den vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlenen Maßnahmen. Da im Rahmen von Gemeinschaftsprojekten in der Regel arbeitsteilig gearbeitet wird, ist es notwendig, dass alle Rundfunkanstalten sich auf eine einheitliche Klassifizierung und die für die jeweiligen Informationsklassen erforderlichen Schutzmaßnahmen verständigen. Um dies zu erreichen, haben AK DSB und CC ISec (Zusammenschluss der Informationssicherheitsbeauftragten der Rundfunkanstalten) in einem ersten Schritt ein gemeinsames Konzept mit vier Schutzklassen und entsprechenden Beispielen erarbeitet, ohne für die

Schutzklassen bereits entsprechende Schutzmaßnahmen definiert zu haben. Unter anderem wurde der Entwurf der JuKo vorgelegt. Sie erachtet eine Klassifizierung zwar grundsätzlich für sinnvoll, plädiert aber dafür, vor einer Verständigung auf ein Raster den damit verbundenen Aufwand und die jeweils an die Kategorien geknüpften Folgen auszuarbeiten. Es bleibt zu hoffen, dass sich die ARD bzw. ARD, ZDF und DLR in absehbarer Zeit auf ein gemeinsames Klassifizierungskonzept einigen. Dadurch könnte der bislang sehr hohe Abstimmungsbedarf bei Gemeinschaftsprojekten deutlich verringert werden.

II. Arbeitsgruppen und übergeordnete Projekte

1. Datenschutz-Koordinatoren

Das Datenschutz-Management des rbb sieht Datenschutz-Koordinatoren vor (Tz. 4.3 der Anlage 2 ‚Datenschutz' der DA Informationsmanagement). Danach hat jede Direktion eine/n Datenschutz-Koordinator:in benannt. Zusätzlich hat auch die Intendanz einen Datenschutz-Koordinator. Die Datenschutz-Koordinator:innen stellen das Bindeglied zwischen der Datenschutzbeauftragten und der jeweiligen Direktion dar.

Im Berichtszeitraum gab es lediglich ein einziges (virtuelles) Treffen der Datenschutzkoordinatoren. Dieses fand am 10.8.2020 gemeinsam mit Mitgliedern des Informationssicherheitskreises statt. Themen waren u. a. Einzelfragen im Zusammenhang mit der DA Informationsmanagement und die Konsequenzen aus dem ‚Schrems II'-Urteil des EuGH.

Die Unterstützungsaktivitäten der Datenschutz-Koordinator:innen fielen im Berichtszeitraum sehr unterschiedlich aus. Besonders hervorzuheben ist der Einsatz des Datenschutz-Koordinators der Programmdirektion, Herrn Uwe Goetz. Dank seiner tatkräftigen Unterstützung konnte ich den Programmkolleg:innen datenschutzrechtliche Anforderungen in Einzelfällen noch besser vermitteln. Auch bei der Erstellung der datenschutzrechtlichen Dokumente für die Meldung einzelner Verfahren zum Verarbeitungsverzeichnis (VVT) wirkte er umfänglich mit.

Für die Zukunft strebt die Datenschutzbeauftragte eine noch engere Zusammenarbeit mit den Datenschutzkoordinator:innen an, die auch häufigere Treffen mit einschließen soll.

2. Beratungstermine in den Redaktionen

Im Rahmen des Projekts zur Umsetzung der DSGVO, dessen Laufzeit im Frühjahr 2019 beendet war, konnten nicht alle Bereiche im rbb individuell angesprochen werden. Das betrifft vor allem die Bereiche der Programmdirektion. Da eine individuelle Ansprache gerade bei grundlegenden Veränderungen sehr wichtig ist, habe ich nach dem Projektende die entsprechenden Informationsmaßnahmen im Bereich der Programmdirektion fortgeführt. Im Berichtsjahr habe ich die nachfolgenden individuellen Beratungstermine zur Umsetzung der DSGVO in den Redaktionen durchgeführt:

- 25.5.2020 Redaktion rbbKultur
- 10.8.2020 Bereich Recherche und Informationsservice
- 9.9.2020 Bereich Programmdokumentation
- 22.9.2020 Sportredaktion
- 23.9.2020 Redaktion rbb Praxis
- 4.11.2020 Redaktionen ‚Täter, Opfer, Polizei', ‚Tier zu liebe' und ‚Gartenzeit'

In diesen Terminen bin ich jeweils individuell auf den Datenschutz bei der Büroorganisation (u. a. Dienstplangestaltung und Dienstreiseplanung) und bei der Durchführung der spezifischen Aufgaben der jeweiligen Redaktion eingegangen. Die Termine dienten zugleich der Identifizierung von Verfahren, die noch in das VVT aufgenommen werden müssen. Diese spezifischen Beratungstermine werden weiter fortgesetzt.

III. IT-Projekte

1. Microsoft 365

Wie berichtet (zuletzt im 16. Tätigkeitsbericht, S. 43 ff.), nutzt der rbb die Kommunikations- und Kollaborationsplattform Microsoft 365. Das cloudbasierte Angebot ermöglicht neue Formen der Zusammenarbeit und hat sich im rbb vielfach bewährt. Die in meinen früheren

Tätigkeitsberichten geäußerten grundsätzlichen datenschutzrechtlichen Bedenken halte ich aber dennoch weiterhin aufrecht. Nach wie vor werden bei der Nutzung von Microsoft 365 eine Vielzahl von Diagnosedaten verarbeitet. Dies kann durch den rbb nicht gänzlich unterbunden werden. Außerdem besteht weiterhin das Risiko, dass US-amerikanische Behörden auf der Grundlage der dortigen Gesetze auf rbb-Daten in der Microsoft-Cloud zugreifen. Um diesem Risiko zu begegnen, hat der rbb die Verarbeitung von streng vertraulichen Daten (z. B. journalistische Recherchedaten aus dem investigativen Bereich) in der Microsoft-Cloud verboten. Ein weiteres Risiko besteht darin, dass der rbb seinen Mitarbeiter:innen und Dritten den vollen Zugriff auf die Daten in der Cloud auch von rbb-fremden Geräten gewährt. Während die rbb-Dienstgeräte stets auf dem neuesten Sicherheitsstand gehalten werden, hat der rbb nur bedingt Einfluss auf den Zustand der für dienstliche Zwecke genutzten Privatgeräte. Zwar schreibt die DA Informationsmanagement in Tz. 3.6 der Anlage 8 ‚IT-Nutzung' vor, dass auf den Privatgeräten die aktuellen Sicherheitsupdates installiert sein müssen. Außerdem muss eine geeignete Software für den Schutz vor Viren und Malware installiert sein. Kontrollieren kann der rbb die Einhaltung dieser Anforderungen aber nicht. Um für den Fall einer Kompromittierung der Privatgeräte eine unerlaubte Weitergabe von sensiblen personenbezogenen Daten zu verhindern, hat der rbb – meiner Forderung entsprechend – Microsoft-Lizenzen mit zusätzlichen Schutzfunktionen angeschafft. Dieser technische Schutz setzt allerdings voraus, dass die Daten zuvor durch die Nutzer:innen entsprechend klassifiziert wurden. Der rbb verlässt sich folglich in doppelter Hinsicht auf die Mitwirkung seiner Mitarbeiter:innen. Diese sind für den Zustand ihrer zu dienstlichen Zwecken genutzten Privatgeräte und für die Klassifizierung der Daten verantwortlich. Im Berichtszeitraum hat sich überdies gezeigt, dass das Sicherheitskonzept nicht in jeder Hinsicht den betrieblichen Notwendigkeiten Rechnung trägt. Eine schnelle Nachbesserung war auch mit externer Unterstützung nicht zu erreichen. Es besteht daher nun die dringende Notwendigkeit, das Sicherheitskonzept noch einmal ganz grundsätzlich auf Tauglichkeit und Praktikabilität zu überprüfen und zu überarbeiten.

Inzwischen hat der rbb weitere Module von Microsoft 365 eingeführt: Hervorzuheben ist der ‚Planner', ein Aufgabenmanagement-Tool, das einem Arbeitsteam wertvolle Unterstützung bieten kann. Er könnte aber auch zur Überwachung der Mitarbeiter:innen genutzt werden, denn er enthält Auswertungsdiagramme, die u. a. zeigen, wie viele Aufgaben die einzelnen

Mitglieder des Teams haben und welche Aufgaben schon überfällig sind. Jedes Teammitglied kann auf alle Daten zugreifen und diese auch verändern. Sämtliche beschriebenen Funktionen können nicht abgestellt werden. Aus diesem Grund spielen verbindliche Nutzungsbedingungen beim Einsatz des ‚Planners' eine wichtige Rolle. Ähnliches gilt für das Modul ‚Forms', mit dem Umfragen durchgeführt und Formulare erstellt werden können. Inzwischen hat sich die in der Dienstvereinbarung zu Microsoft 365 vorgesehene AG Microsoft 365 gebildet. Ihr gehören Mitarbeiter:innen der HA Mediensysteme und IT (HA MIT), Mitglieder des Personalrats, die Schwerbehindertenvertretung, der Informationssicherheitsbeauftragte und die Datenschutzbeauftragte an. Die AG tagt regelmäßig mindestens einmal im Monat per Videokonferenz. Die Mitarbeiter:innen der HA MIT informieren darin über durch Microsoft vorgenommene Veränderungen und Erweiterungen am System und über die beabsichtigte Einführung weiterer Module. Die AG definiert gemeinsam die Möglichkeiten und Grenzen des Einsatzes der einzelnen Module und legt die Nutzungsbedingungen fest. Die Nutzungsbedingungen werden nach Beschlussfassung durch die Geschäftsleitung und Veröffentlichung im Intranet verbindlich.

2. SAP- Prozessharmonisierung – Projekt „(D)ein SAP"

Über den Stand des ARD-Projekts „(D)ein SAP" hatte ich zuletzt in meinem letzten Tätigkeitsbericht informiert (16. Tätigkeitsbericht, S. 38 f.). Der Zeitplan hat sich inzwischen erneut verschoben. Nach einem umfassenden Projekt-Review steht fest, dass der 1.1.2022 als Starttermin für Cluster 1 (beinhaltet die Module Finanzen, Dienstreisen, Controlling, Beschaffung/Vertragswesen/Warenwirtschaft und den Personal-Ministamm) bei allen elf am Projekt beteiligten Rundfunkanstalten und der GSEA Zentraler Beitragsservice (ZBS) nicht gehalten werden kann. Aktuell erstellt das Projekt nach Empfehlung des Projekt-Reviews und im Auftrag des Lenkungsausschusses eine neuerliche Feinplanung, in deren Ergebnis der genaue Kosten- und Ressourcenbedarf für das weitere Vorgehen ermittelt werden soll. Geprüft wird in diesem Zusammenhang ein Produktivstart von Cluster 1 in zwei Wellen. Danach würde eine Gruppe von Rundfunkanstalten mit Cluster 1 zum 1.1.2023 starten. Eine zweite Gruppe würde zum 1.1.2024 folgen. Die Projektarbeiten laufen trotz der Review-Ergebnisse mit Priorität A weiter, um zusätzlichen Zeitverzug zu verhindern.

Die datenschutzrechtliche Prüfung der neuen S/4-HANA-Landschaft erfolgt für die einzelnen Module in den Rundfunkanstalten nach dem Federführungsprinzip durch die jeweiligen Datenschutzbeauftragten. Allerdings entbindet mich dies nicht davon, sämtliche Dokumente zu prüfen, zumal die Module zum Teil zusammengehören bzw. es zumindest Schnittstellen gibt und beim rbb Besonderheiten bestehen können.

Meine Federführung betrifft dabei das vom rbb als Prozesseigner verantwortete Modul Beschaffung/Vertragswesen/Warenwirtschaft. In diesem Zusammenhang habe ich zunächst an der Erarbeitung der datenschutzrelevanten Anforderungen und Dokumente für die EU-Ausschreibung eines Cloud-Services (‚Software as a service') für das E-Procurement (elektronische Bedarfsanmeldung von Handelswaren und Dienstleistungen) mitgewirkt. Inzwischen wurde der Zuschlag an ein Bieterkonsortium mit der Software JAEGGER vergeben.

Auch habe ich im Rahmen dieser Federführung alle vom Projekt für die Integrationstests des Moduls ‚Beschaffung' mit Echtdaten vorgelegten Unterlagen geprüft. Aus meinen umfangreichen Anmerkungen und den nicht minder umfangreichen Rückmeldungen meiner Kolleginnen und Kollegen zu den anderen Modulen aus Cluster 1 hat das Projekt Aufgaben-Backlogs erstellt, die das Projekt nun Schritt für Schritt abarbeitet. Dazu gehört das Vorgehen bei der Migration der Stammdatensätze externer Geschäftspartner von den Altsystemen der Rundfunkanstalten, also auch aus den Systemen des rbb, in die neue S4/HANA-Landschaft. Hier arbeitet das Projekt aktuell an der Umsetzung unserer ebenfalls umfangreichen Anmerkungen. Außerdem habe ich das Löschkonzept für den SAP Solution Manager (‚SolMan') geprüft. Der ‚SolMan' ist das zentrale Tool, mit dem alle Anwendungen innerhalb (D)ein SAP über ihre gesamte Lebensdauer hinweg von der Entwicklung über die Testung bis zum Betrieb und danach zur Weiterentwicklung gesteuert und dokumentiert werden. Während der aktuellen Projektarbeit wird er zunächst zielgerichtet für die Entwicklungsarbeit eingesetzt.

Da das ‚SolMan'-System als zentrales System vor allen anderen SAP-Anwendungen und Systemen aufgebaut und produktiv genommen werden muss, hat das Projekt eine Sicherheitsüberprüfung des ‚SolMan' durch die Fa. PwC veranlasst. Diese fand im September 2020 statt. Im Ergebnis fand PwC zahlreiche technische und konzeptionelle Mängel, die jetzt behoben werden müssen.

3. Telefonanlage Open Scape und Unified Communication

In meinen letzten Tätigkeitsberichten habe ich über die probeweise Einführung des Kommunikationsdienstes ‚Unified Communication' (UC) berichtet (16. Tätigkeitsbericht, S. 53). UC ist eine Anwendung des neuen Voice over IP-Telekommunikationssystems (Open Scape Voice). Dieses neue Telefonsystem wird die bestehenden ISDN-IP Hybrid-Kommunikationsysteme im rbb schrittweise ablösen. UC beschreibt die Integration von unterschiedlichen Kommunikationsmedien in einer einheitlichen Anwendungsumgebung. Die Idee hinter UC ist, durch eine Zusammenführung aller Kommunikationsdienste und ihre Integration in die Geschäftsanwendungen die Kommunikation innerhalb des Unternehmens effektiver zu gestalten und die Erreichbarkeit von Kommunikationspartnern zu verbessern. Zusätzlich zu den Funktionen einer herkömmlichen Telefonanlage bietet UC verschiedene weitere Leistungsmerkmale, die u. a. Telefonkonferenzen und Videotelefonie sowie Chat-Funktionen umfassen. Nach der Einführung von Microsoft 365 bestehen nun zum Teil deckungsgleiche Leistungsmerkmale von UC und Microsoft 365 nebeneinander. Dessen ungeachtet strebt die HA MIT jetzt nach einer mehrjährigen Test- und Probephase den Regelbetrieb für die neue TK-Anlage und UC an. Aus diesem Grund kamen die Projektverantwortlichen im vierten Quartal 2020 auf mich zu. Alle zur datenschutzrechtlichen Freigabe erforderlichen Dokumente wurden in dieser späten Phase in Zusammenarbeit mit mir gemeinsam erstellt. Im Januar 2021 konnte seitens der Datenschutzbeauftragten ‚grünes Licht' für den Regelbetrieb erteilt und das Verfahren in das VVT aufgenommen werden. Auch die Verhandlungen der Geschäftsleitung mit dem Personalrat über eine Dienstvereinbarung zur neuen TK-Anlage einschließlich UC sind inzwischen abgeschlossen. Zur Enttäuschung der Datenschutzbeauftragten blieben in dem dem Personalrat im Januar 2021 vorgelegten Entwurf der Dienstvereinbarung die mit den Projektverantwortlichen getroffenen datenschutzrechtlichen Festlegungen unberücksichtigt. Der Entwurf war bereits im Sommer 2020 mit dem Vorgänger-Personalrat verhandelt und seitens des rbb nicht mehr ergänzt worden. Aktuell liegt der Entwurf der Dienstvereinbarung dem Justitiariat zur finalen Prüfung vor.

4. Abschaffung des ARD-Konferenzsystems

Zum 30.11.2020 ist aus wirtschaftlichen Gründen das ARD-Konferenzsystem beim rbb, wie in den meisten anderen Rundfunkanstalten, abgeschaltet worden. Die vorhandenen Lizenzen bleiben dem NDR und den Gemeinschaftseinrichtungen, die noch kein eigenes Videokonferenzsystem angeschafft haben, vorbehalten. Nunmehr gibt es beim rbb keine Alternative mehr zur Nutzung des Videokonferenzsystems Microsoft Teams. Mit Abschaffung des ARD-Konferenzsystems hat die ARD einen weiteren Teil seiner digitalen Souveränität aufgegeben. Mit dieser Entscheidung haben sich die zuständigen technischen Gremien auch über die Forderungen von AK DSB und RDSK hinweggesetzt, für Videokonferenzen mit streng vertraulichem Inhalt neben Microsoft Teams ein eigenes System beizubehalten. Streng vertrauliche personenbezogene Daten müssen vollständig vor dem Zugriff Externer – einschließlich dem des externen Dienstleisters – geschützt sein. Dies gilt insbesondere für externe Dienstleister, die ihren Sitz außerhalb der EU haben und die Anforderungen der DSGVO nicht vollständig erfüllen können. Kann ein Zugriff des externen Dienstleisters nicht vollständig ausgeschlossen werden (wie bei Microsoft Teams), so muss die Rundfunkanstalt ggf. im Verbund mit anderen Rundfunkanstalten für diese streng vertraulichen Daten ein eigenes System betreiben (s. dazu auch „Datenschutzrechtliche Eckpunkte zum Einsatz von Kollaborationssystemen“ der RDSK, Stand Februar 2021, Anlage 3).

5. Sicherheitskonzept für mobile Endgeräte

Mobile Endgeräte werden den rbb-Mitarbeiter:innen zur Verfügung gestellt, wenn dies für dienstliche Zwecke notwendig ist. Die Geräte werden von der HA MIT beschafft und verwaltet. Alle mobilen Endgeräte werden im rbb durch das Mobile Device Management (= Zentrale Verwaltung der Geräte) Mobileiron verwaltet.

Schon Ende 2018 hatten sich einige MoJos (Mobile Journalists) an mich gewandt, weil sie Sorge hatten, dass bei der Nutzung der Dienstgeräte ihre Nutzungsdaten wie Sprache über die Sprachfunktion Siri und Ortungsdaten über die Navigationssoftware unkontrolliert an Dritte abfließen könnten (16. Tätigkeitsbericht, S. 67 ff.). Gemeinsam mit den Kollegen aus der

Informationssicherheit hatte ich gegenüber der HA MIT eine datenschutzfreundliche Konfiguration sowie datenschutzfreundliche Voreinstellungen der Dienstgeräte eingefordert. Allerdings zeigte sich in der Folge, dass es ganz unterschiedliche Einsatzbereiche mit unterschiedlichen Anforderungen an die Konfiguration der mobilen Dienstgeräte gibt. Daraufhin haben wir zunächst einmal die Nutzergruppen und die jeweiligen Bedarfe identifiziert.

Folgende Gerätegruppen sind vorhanden:

- Dienstgerät (personenbezogene Geräte)
- MoJo (Pool-Geräte für mobile Journalisten)
- EB-Einheiten (einer EB-Einheit fest zugeordnet)
- Moderations-iPads (Pool-Geräte)
- Steuerungs-iPads (Pool-Geräte)

Auf dieser Basis haben die Kollegen aus der Informationssicherheit in Abstimmung mit mir ein Sicherheitskonzept erarbeitet, das sowohl den jeweils unterschiedlichen Anforderungen als auch den Sicherheitsaspekten und dem Datenschutz optimal Rechnung trägt. Anfang Dezember 2020 haben wir das Konzept der Leiterin der HA MIT vorgestellt. Im Rahmen der Präsentation haben wir auch die Bedeutung eines Mobile Device Managements hervorgehoben. Nur durch die zentrale Verwaltung der Geräte kann sichergestellt werden, dass die Endgeräte einheitliche Sicherheitsstandards aufweisen. Das Sicherheitskonzept ist nun verbindlich und wird konsequent umgesetzt.

6. Mobile SAP-Nutzung

Im Zusammenhang mit der Umstellung auf die Arbeit im Homeoffice hat der rbb im März 2020 beim Personalrat einen Antrag auf Zustimmung zur mobilen SAP-Nutzung gestellt. Dem ging eine Konsultation des Informationssicherheitsbeauftragten und der Datenschutzbeauftragten voraus, die bestätigten, dass die mobile Nutzung auf der Grundlage von TZ. 3.8 von Anlage 8 der DA Informationsmanagement zulässig ist. Danach erfolgt die mobile SAP-Nutzung ausschließlich mit Geräten des rbb über eine verschlüsselte VPN-Verbindung. Der Personalrat hat

zunächst nur eine befristete Zustimmung bis zum 31.12.2020 erteilt. Nachdem klar wurde, dass die Notwendigkeit von mobiler Arbeit langfristig weiterbestehen wird, hat der rbb am 19.12.2020 mit meiner Zustimmung eine unbefristete Zustimmung zur mobilen SAP-Nutzung beantragt. Dem hat der Personalrat auf seiner Sitzung am 22.12.2020 entsprochen.

7. Print at Work – Druckermanagementsystem

Auch über das neue Druckermanagementsystem habe ich schon in meinen letzten Tätigkeitsberichten informiert (zuletzt 16. Tätigkeitsbericht, S. 52). Aus 1.200 Druckern und Multifunktionsgeräten unterschiedlichster Art wurden 120 Druckerinseln mit insgesamt rund 480 Druckern und Multifunktionsgeräten von einer einzigen Firma in fünf verschiedenen Ausführungen. Die Druckerinseln befinden sich in separaten Räumen, an zentralen Stellen in Großraumbüros und in Küchen. Im Herbst 2020 konnte der Konsolidierungsprozess erfolgreich abgeschlossen werden. Seit Oktober 2020 befindet sich das System im Regelbetrieb. Aus Datenschutzsicht zu begrüßen ist die Möglichkeit des vertraulichen Druckens. Dabei können beliebig viele Druckaufträge online an einen Drucker abgeschickt und erst später vor Ort zum Druck freigegeben werden. Zur Authentifizierung muss der Hausausweis an ein Lesegerät gehalten werden. Die Datei selbst bleibt bis zur Abholung auf einem sicheren Server. Ursprünglich war vorgesehen, dass der Druckauftrag automatisch nach 24 Stunden gelöscht wird, wenn ein Druckauftrag bis dahin nicht ausgelöst wurde. Die Erfahrung zeigte, dass diese Frist angesichts der aktuellen Homeoffice-Regel zu kurz war. Mit Zustimmung der Datenschutzbeauftragten wurde daher entschieden, die Druckaufträge bis auf weiteres sieben Tage auf dem Server zu belassen.

8. ARD-Servicedesk (OTRS)

Im Rahmen der ARD-Strukturreform wurde beschlossen, einen zentralen Servicedesk für sämtliche ARD-Anstalten und das Deutschlandradio zu etablieren, um Synergie- und Einspareffekte zu erzielen. Der Bayerische Rundfunk (BR) hat in seiner Funktion als Lead-Buyer einen externen Dienstleister für die ARD ausgeschrieben. Die Firma Datagroup hat den Zuschlag

erhalten und seitdem tritt eine Landesrundfunkanstalt nach der anderen dem ARD-Servicedesk bei.

Der ARD-Servicedesk nutzt zur Kommunikation das Ticketsystem OTRS, mit dem die eingehenden Anfragen und Störmeldungen über verschiedene Wege (Telefon, E-Mail, Webformular, Chat) systematisch erfasst, klassifiziert, an die zuständige Stelle weitergeleitet, bearbeitet und dokumentiert werden.

Vom BR wurde ein Sicherheitskonzept erarbeitet, welches für alle Rundfunkanstalten gilt.

Zum 1.7.2021 wird der rbb dem zentralen Servicedesk beitreten. Das HSB und das IVZ nehmen schon seit Februar 2021 daran teil. Bei der Erstellung der datenschutzrechtlichen Dokumente gab es zunächst Verzögerungen. Nun liegen aber alle notwendigen Unterlagen vor, weshalb das Verfahren in Kürze in das VVT aufgenommen werden kann.

9. Ausweis- und Berechtigungsmanagementsystem

Im Rahmen des Projektes ‚Sicherheitskonzept' wird die Sicherheit in den Gebäuden und auf dem Betriebsgelände des rbb durch die Umsetzung baulicher, technischer und organisatorischer Maßnahmen kontinuierlich erhöht. Schon zu Beginn des Jahres 2020 konnte das neue Ausweis- und Berechtigungsmanagementsystem in den Regelbetrieb gehen (16. Tätigkeitsbericht, S. 49 ff.). Im Berichtszeitraum wurden weitere Außenzugänge auf den Betriebsgeländen in Berlin und Potsdam mit elektronischen Zutrittssicherungen versehen. Eine detaillierte Stellungnahme der Datenschutzbeauftragten war dazu nicht notwendig, da das bestehende Zutrittskontrollsystem lediglich um technische Komponenten erweitert wurde.

10. Neues Besucheranmeldesystem

Wie berichtet (16. Tätigkeitsbericht, S. 51), war es durch die Einführung der Zutrittskontrollanlagen notwendig geworden, auch das Verfahren für die Anmeldung von Besucher:innen, Auszubildenden, Praktikant:innen und neuen freien sowie neuen festen Mitarbeiter:innen

neu zu gestalten. Für die Empfangsanmeldung hat der rbb daher ein browserbasiertes Tool angeschafft, über welches Besucher von rbb-Mitarbeiter:innen angemeldet werden können. Dem ursprünglich bis zum 22.5.2020 geplanten Probebetrieb konnte ich zustimmen, nachdem alle für die Einführung notwendigen Dokumente vorlagen. Der Probebetrieb wurde mehrfach verlängert. In dieser Zeit ist das bestehende Betriebskonzept laufend überarbeitet worden. Die vorerst letzte Verlängerung des Probebetriebs endete am 30.4.2021, eine weitere wurde beantragt.

11. Datenschutzerklärung für die Videokameras

Wie im letzten Tätigkeitsbericht mitgeteilt (16. Tätigkeitsbericht, S. 51) nutzt der rbb auf seinem Gelände zum Schutz seines Eigentums vor Diebstahl und Vandalismus sowie vor weiteren Bedrohungen Videokameras. Zur Erfüllung des datenschutzrechtlichen Transparenzgrundsatzes müssen an den Videokameras jeweils Datenschutzerklärungen angebracht sein. Im Juli 2020 konnten die Beschilderungen mit der mit mir zuvor abgestimmten Datenschutzerklärung an den Immobilien des rbb sowie im ARD-Hauptstadtstudio durch die Abteilung Intrastruktur abgeschlossen werden.

IV. Beschäftigtendatenschutz

1. Datenschutzfragen im Zusammenhang mit den Corona-bedingten Maßnahmen

1.1. Einsatz der Corona-Warn-App

Seit dem 16.6.2020 ist in Deutschland die Corona-Warn-App zum Download verfügbar. Mithilfe dieser App sollen Kontaktketten von Corona-Infizierten nachverfolgt werden. Das Ziel: Menschen, die in Kontakt mit positiv getesteten Personen waren, sollen von der App gewarnt werden, dass sie sich bei der infizierten Person angesteckt haben könnten. Die Corona-Warn-App wurde im Auftrag der Bundesregierung von SAP und der Telekom-Tochter T-Systems entwickelt. Sie basiert auf einem dezentralen Ansatz. Begegnungen werden auf jedem einzelnen

Gerät gespeichert und nicht zentral, z. B. auf Servern. Dies ist aus Datenschutzsicht sehr zu begrüßen. Nicht erfasst werden überdies Standort oder Identität der Anwender:innen. Anbieter dieser App ist das Robert-Koch-Institut (RKI). Die Nutzung der App ist freiwillig. Auf Nachfrage habe ich die Installation der Corona-Warn-App befürwortet, aber zugleich darauf hingewiesen, dass es zur Wahrung des Freiwilligkeitsprinzips keine Verpflichtung zur Installation der App im rbb geben darf, auch nicht auf den rbb-Dienstgeräten.

1.2. Anwesenheitsdokumentation für Gäste in den Kantinen

Durch entsprechende Infektionsschutzverordnungen in den Bundesländern sind unter anderem Kantinenbetreiber dazu verpflichtet, die Daten ihrer Besucher:innen zur Kontaktnachverfolgung zu dokumentieren. Das Verfahren zur Anwesenheitsdokumentation und die Datenschutzerklärungen wurden vorsorglich mit der rbb-Datenschutzbeauftragten abgestimmt, obschon allein die Pächter der Kantinen für die Ordnungsmäßigkeit der Datenverarbeitung im Zusammenhang mit der Anwesenheitsdokumentation verantwortlich im datenschutzrechtlichen Sinne sind.

1.3. Umgang mit Corona-Tests und Testergebnissen

Seit Februar 2021 können die rbb-Beschäftigten Corona-Selbsttests durchführen. Das Angebot richtet sich an alle, die regelmäßig vor Ort im Sender arbeiten und ist ohne Anmeldung nutzbar. Die Selbsttests werden durch eine externe Fachfirma begleitet. Bei der Festlegung des Verfahrens und der Formulierung der Datenschutzerklärung habe ich die Kolleginnen aus dem Gesundheitsmanagement des rbb beraten. Mit der begleitenden Fachfirma wurde eine Vereinbarung zur Auftragsverarbeitung abgeschlossen. Die Selbsttests sind freiwillig.

Im Bereich der Maske müssen die Mitarbeiter:innen, da es sich dort um körpernahe Dienstleistungen handelt, einen tagesaktuellen negativen Corona-Test vorweisen. Außerdem muss es in diesem Bereich auch eine Anwesenheitsdokumentation geben. Über die Art und Weise

der Führung des Nachweises hat es anfänglich einige Irritationen gegeben. Die Datenschutzbeauftragte wurde erst zu einem relativ späten Zeitpunkt konsultiert. Aktuell finden letzte Abstimmungen zum Workflow statt. Die Abstimmungen werden dadurch erschwert, dass sich durch häufige Änderungen der Infektionsschutzverordnung immer neue Anforderungen ergeben. Aus Sicht der Datenschutzbeauftragten kommt der Gestaltung eines datenschutzrechtlich sauberen und transparenten Verfahrens hohe Priorität zu, da es um die Verarbeitung von sensiblen Gesundheitsdaten geht.

2. SAP xSS-Anwendung

Seit Herbst 2019 befindet sich SAP xSS mit den Anwendungen Abwesenheitsmanagement und Arbeitszeitmanagement im Probebetrieb (s. 16. Tätigkeitsbericht, S. 54 f.). Die anfänglichen datenschutzrechtlich relevanten Probleme konnten inzwischen behoben werden: Abgeschlossene Fehlmeldungen sind nicht mehr bis zum 2.9.2019, sondern nur noch für zwei Monate rückwirkend sichtbar. Der Teamkalender ist nicht mehr rückwirkend ab 1.1.2019, sondern für alle nur noch für das laufende und das Vorjahr einsehbar. Einzige Ausnahme: Wenn eine Abwesenheit über den Jahreswechsel andauert, wird sie vollständig angezeigt und nicht etwa zum 31.12. des betreffenden Jahres abgeschnitten. In diesen Fällen kann man über das Vorjahr hinaus in den Dezember des Vorvorjahres schauen.

Seit Juni 2020 wird SAP xSS auch dafür genutzt, den Arbeitnehmer:innen ihre Gehaltsabrechnungen auf elektronischem Wege zur Verfügung zu stellen. Auf der Startseite von SAP xSS steht jetzt die Kachel ‚Meine Entgeltnachweise' zur Verfügung, über die die Gehaltsabrechnungen abgerufen werden können. Diese werden aus dem SAP-Personalverarbeitungssystem individualisiert in die neue Anwendung gespiegelt und entsprechen damit eins zu eins denjenigen Gehaltsabrechnungen, die die Beschäftigten zuvor in Papierform erhalten haben. Bestimmte Personengruppen wie Arbeitnehmer:innen in Elternzeit, Langzeiterkrankte etc. erhalten ihre Gehaltsabrechnungen nach wie vor auf dem Postweg. Auf der Basis der positiven Stellungnahme des Informationssicherheitsbeauftragten zum Einsatz von SAP xSS für die elektronischen Gehaltsabrechnungen konnte ich den VVT-Erfassungsbogen gemeinsam mit

der Projektleiterin aus der HA Personal ausfüllen und dem Probebetrieb zustimmen. Die Anwendung ‚Meine Entgeltnachweise' hat von Anfang an problemlos und störungsfrei funktioniert. In Abstimmung mit dem Personalrat wurde für alle Anwendungen in xSS der Probebetrieb bis zum 31.1.2022 verlängert.

3. Dispositionssystem Malu in der Hörfunk-Disposition

Zur Disposition von Personal- und Sachmitteln werden im rbb leider nach wie vor unterschiedliche Verfahren mit unterschiedlichen Softwareprogrammen praktiziert (s. 16. Tätigkeitsbericht S. 55 f.). Für das Dispositionssystem Malu gibt es nach wie vor kein Löschkonzept. Außerdem ist das Berechtigungskonzept weiterhin fehlerhaft und die technischen Auswertungsmöglichkeiten gehen immer noch zu weit. Sollte das System im laufenden Jahr nicht abgeschaltet werden, behalte ich mir entsprechende Maßnahmen vor.

4. Meldeportal des neuen Versicherungsmaklers der ARD

Wie berichtet, hat der Norddeutsche Rundfunk (NDR) mit Wirkung auch für die anderen ARD-Rundfunkanstalten einen Vertrag mit einem neuen Versicherungsmakler abgeschlossen. Betreut werden die Sach- und Transportversicherungen sowie die Haftpflichtversicherungen der Rundfunkanstalten. Der Versicherungsmakler hat den Rundfunkanstalten ein Tool zur Verfügung gestellt, über das die Rundfunkanstalten ihre Schäden eigenständig an den Versicherungsmakler melden können. Der rbb war bislang eine der wenigen Rundfunkanstalten, die dieses Tool nicht nutzten. Ausschlaggebend war die Tatsache, dass die Versicherungsabteilungen der beteiligten Rundfunkanstalten in bestimmten Fallkonstellationen auch die Schadensmeldungen der anderen Häuser einsehen konnten (16. Tätigkeitsbericht, S. 56 f.). Inzwischen hat der rbb einen Weg gefunden, diese Fälle für die rbb-Beschäftigten auszuschließen. Anders als in anderen Rundfunkanstalten geben im rbb nur geschulte Mitarbeiter:innen des zuständigen Fachbereichs die Meldungen in das Schadensportal ein. Nach dieser Klärung konnte die Datenschutzbeauftragte der Nutzung des Portals zustimmen und das Verfahren in das VVT aufnehmen.

5. Neue Lernplattform der ARD.ZDF Medienakademie

Anfang 2020 hat die ARD.ZDF Medienakademie allen beteiligten Rundfunkanstalten eine neue Lernplattform zur Verfügung gestellt. Diese Lernplattform enthält die Onlinekurse der Medienakademie und deren Schulungsmaterial. Die Plattform ermöglicht es den beteiligten Rundfunkanstalten aber auch, ihren Beschäftigten eigene Kurse und Kursinhalte auf der Plattform anzubieten. Die Plattform ist mandantenfähig, das heißt, dass jede Rundfunkanstalt einen eigenen Bereich darauf hat, den sie selbst verwaltet. Die Lernplattform ermöglicht es den Beschäftigten u. a., ihren jeweiligen Lernfortschritt abzuspeichern und Zertifikate erfolgreich abgeschlossener Kurse auszudrucken.

Für mich etwas überraschend geht die Medienakademie davon aus, vollumfänglich selbst Verantwortlicher im datenschutzrechtlichen Sinne und nicht Auftragsverarbeiter für die Rundfunkanstalten zu sein. Dies wird auch von den Datenschutzbeauftragten der anderen Rundfunkanstalten für zutreffend gehalten, so dass wir nun auch für den rbb von dieser rechtlichen Konstruktion ausgehen. Allerdings habe ich darauf geachtet, dass alle datenschutzrechtlich relevanten Dokumente wie Betriebskonzept, Informationssicherheitskonzept, VVT-Erfassungsbogen und die Datenschutzerklärung dem rbb-Standard entsprechen. Ausnahmsweise habe ich aus Transparenzgründen die Dokumente auch in unser VVT aufgenommen, in dem ansonsten ausschließlich rbb-eigene Verfahren und diejenigen Verfahren der rechtlich unselbstständigen Gemeinschaftseinrichtungen, für die der rbb Federführer ist, dokumentiert sind.

Inzwischen nutzt der rbb die Lernplattform sehr intensiv. Dabei muss aus Sicht der Datenschutzbeauftragten darauf geachtet werden, dass verbindliche Dienstanweisungen und Nutzungsbedingungen nicht exklusiv auf dieser externen Plattform, sondern zusätzlich leicht auffindbar im rbb-Intranet vorgehalten werden. Anderenfalls kann der rbb nicht davon ausgehen, dass diese verbindlichen Vorgaben auch tatsächlich als solche von allen Beschäftigten wahrgenommen werden.

6. Digitalisierung der Personalakte

Bislang erfolgt die Personalaktenführung der festen und freien Mitarbeiter:innen in Papierform. Auch für die Versorgungsempfänger:innen werden Papierakten vorgehalten. In den Personalakten werden alle für das Beschäftigungsverhältnis relevanten Daten für die Mitarbeiter:innen gesammelt. Die Ablage findet manuell statt. Die Entfernung der Unterlagen nach Ablauf der Aufbewahrungsfrist erfolgt ebenfalls manuell. Die Beschäftigten und ihre Vorgesetzen erhalten unter den in der DA Personalaktenführung genannten Voraussetzungen Einblick in die Personalakte. Dies erfolgt innerhalb der Räumlichkeiten der HA Personal.

Die Personalaktenführung erfordert einen sehr hohen manuellen Aufwand. Alle Unterlagen müssen per Hand hinzugefügt und entfernt werden. So kann es vorkommen, dass Unterlagen nicht zeitnah in die Personalakte aufgenommen oder nicht mit Ablauf der Aufbewahrungsfrist entfernt werden. Hinzu kommt, dass die Personalakten einen enormen Platzbedarf haben und im Fall eines Wasser- oder Feuerschadens unwiederbringlich zerstört werden könnten, da es keine Kopie gibt. Auf diese Risiken hatte ich in der Vergangenheit wiederholt hingewiesen und entsprechende Maßnahmen zur Begrenzung eingefordert.

Im Februar 2021 informierte mich die HA Personal darüber, dass sie beabsichtige, zukünftig digitale Personalakten zu führen. Dadurch können die manuellen Vorgänge reduziert und die Personalakteneinsicht erleichtert werden. Das Dokumentenmanagementsystem zur Aufbewahrung der Personalakten solle dabei in das existierende SAP-System integriert werden.

Erwartungsgemäß hat der Informationssicherheitsbeauftragte die Schutzziele Vertraulichkeit und Integrität der Personalakten als sehr hoch eingestuft. Die Anforderungen an die Verfügbarkeit wurden mit hoch bewertet. Auf dieser Basis wurde ein Unternehmen mit der Digitalisierung der Personalakten beauftragt, dessen technische und organisatorische Maßnahmen und dessen Sicherheitskonzept für den Umgang mit den Akten beim Transport, Lagerung sowie Verarbeitung dem sehr hohen Schutzbedarf der Personalakten entspricht. Es handelt sich dabei um denselben Dienstleister, der auch schon die Lizenzakten des rbb digitalisiert hat. Der rbb hat eine Vereinbarung zur Auftragsdatenverarbeitung mit dem Dienstleister abgeschlossen. Nach Prüfung aller Dokumente konnte ich dem Digitalisierungsverfahren zustimmen und

dies in das VVT aufnehmen. Mit der HA Personal habe ich verabredet, dass ich über den ersten Termin zum Abtransport von Personalakten durch den Dienstleister zum Zweck der Digitalisierung informiert werde. Ich beabsichtige, dieses Verfahren persönlich zu begleiten und mich von der Ordnungsgemäßheit zu überzeugen.

Die eigentliche Aktenführung im neuen Dokumentenmanagementsystem muss noch mit mir abgestimmt werden. Dafür wird auch eine Anpassung der DA zur Führung der Personalakten erforderlich sein.

V. Datenschutz bei der Produktion und im Programm

1. KI-Projekte

Künstliche Intelligenz (KI) gewinnt bei der Produktion redaktioneller Inhalte zunehmend an Bedeutung. Im Zusammenhang mit der Nutzung von KI stellen sich zahlreiche datenschutzrechtliche Fragen, zumal dabei auch biometrische Daten verarbeitet werden können, die einem besonderen rechtlichen Schutz unterliegen (Art. 9 DSGVO). In der Abteilung Technisches Innovationsmanagement laufen insgesamt sechs KI-Projekte. Bislang ist die Datenschutzbeauftragte in zwei Projekte intensiver einbezogen worden.

1.1. Materialerkennung

Ziel der Materialerkennung mit Hilfe von KI ist es, einen schnelleren Überblick über die Vielzahl von neuem Bewegtbildmaterial zu bekommen. Dabei analysiert ein KI-basiertes System das Video-Material hinsichtlich verschiedener Parameter. Über eine einfache Such- und Auswahlfunktion können die Redaktionen entscheiden, welches Material relevant ist.

Seit Anfang März 2021 führt das Technische Innovationsmanagement einen ‚Proof of Concept' (POC) für die Video-Materialerkennung mit Hilfe von KI durch. Dafür wird zunächst eine Materialdatenbank zur Personen- und Landmarkenerkennung aufgebaut. Die technische Entwicklung erfolgt zusammen mit einem Freiburger Unternehmen und dessen KI-Tool ‚DeepVA'.

Für das Erstellen der Materialdatenbank liegt der Fokus auf dem teilautomatisierten Workflow der Auslese der sogenannten Bauchbinden. Als Bauchbinde bezeichnet man eine Einblendung am unteren Bildrand, die den Namen sowie (optional) eine Einordnung der Person im Sendungskontext (wie z. B. Funktion, Beruf u. Ä.) angibt. Dazu wird gesendetes rbb-Nachrichtenmaterial manuell in das Tool ‚DeepVA' geladen, um dort einen Analyseprozess zu durchlaufen. Gesichter und Texte aus den Bauchbinden werden in die Datenbank eingespeist. Diese Informationen bilden die Grundlage für den Lernprozess der KI. Zusätzlich kann das Tool manuell mit Bildmaterial von Sehenswürdigkeiten und Gebäuden erweitert werden.

Der BR hat schon vor dem rbb eine entsprechende Trainingsdatenbank mit Hilfe des Tools ‚DeepVA' aufgebaut. Zum Schutz des Persönlichkeitsrechts der abgebildeten Personen wurden hier u. a. folgende Maßnahmen ergriffen: Gespeichert wurden ausschließlich Bilder mit den dazugehörenden Namen von Personen des öffentlichen Lebens, Kinder und Patienten wurden ausdrücklich ausgenommen. Der Aufbau der Trainingsdatenbank wurde zudem durch sogenannte KI-Manager begleitet, die die Einhaltung dieser Einschränkungen überwacht haben.

Das Technische Informationsmanagement ist meiner Empfehlung gefolgt und lehnt sich bei der Durchführung des POC im rbb an die Festlegungen des BR an. Bisher funktioniert die Erkennung der Gesichter und die Extraktion der Bauchbinden wie erwartet gut, so dass die Materialdatenbank kontinuierlich wächst. Allerdings bedeutet die notwendige manuelle Beurteilung des KI-Trainingsmaterials und die Bearbeitung des Datensets einen zusätzlichen Arbeitsaufwand für die Mitarbeiter:innen der Archive. Im weiteren Verlauf des POC werden die Ergebnisse mit Redaktionen evaluiert und die KI-Modelle angewendet, um die Auffindbarkeit von Personen und Objekten zu ermöglichen. Mit dem Technischen Innovationsmanagement ist verabredet, dass ich in die Evaluation einbezogen werde.

1.2. Text-to-Speech

Das Projekt ‚Text-to-Speech' (TTS) hat die Entwicklung eines Tools zum Ziel, das automatisch Text-Daten aus den rbb-Systemen entgegennimmt, diese Texte mittels Sprachsynthese in

Audios umwandelt und diese Audio-Dateien in Richtung der rbb-eigenen Veröffentlichungssysteme weitergibt, speziell an das Content-Management-System (CMS) für die Inforadio Smartphone-App und den Alexa-Skill. Geplant ist die Verwendung derartiger Audios in den Randzeiten. In einem POC soll dabei der Nutzen dieser KI-Technik getestet werden. Als Plattform wird die Azure-Cloud von Microsoft genutzt. Ein Berliner Unternehmen ist als Auftragsverarbeiter mit der technischen Umsetzung betraut. Mit dem Unternehmen wurde eine Vereinbarung zur Auftragsverarbeitung abgeschlossen. Bei den Texten für die Sprachsynthese handelt es sich um Verkehrs- und Wettermeldungen. Die Übertragung aus den rbb-Systemen in die Azure-Cloud erfolgt über eine verschlüsselte Verbindung. Innerhalb der Azure Plattform erfolgt mit Hilfe des Speech-Dienstes die Erstellung von Audiofiles. Diese werden wiederum über eine verschlüsselte FTP-Verbindung auf dem rbb-FTP-Server abgelegt und dort mit Hilfe des Online-CMS in die rbb-Webangebote von Inforadio eingebunden. Innerhalb des POC findet keine Anbindung an die rbb-Azure-AD statt. Es wird zunächst mit Test-Accounts gearbeitet.

Nachdem der POC bereits initiiert war, trat die Projektleitung mit einem zusätzlichen Vorhaben an mich heran: Die Redaktion von Inforadio beabsichtigt, eine eigene Stimme zu produzieren, damit die Audios als originäre rbb- bzw. Inforadio-Nachrichten akustisch erkennbar sind. Zur Stimmproduktion wird die Sprecherin eine Anzahl von Mustersätzen einsprechen. Diese werden aufgezeichnet und von der KI später analysiert und zerlegt und in einem Stimm-Modell vorgehalten, inklusive aller Charakteristika wie Klangfarbe und Aussprache. Wird dieses Stimm-Modell später im TTS-Prozess eingesetzt, werden die zerlegten Klangkurven je nach Text-Input neu zusammengesetzt und es entstehen Audios, die klingen, als ob die Sprecherin persönlich die Texte eingesprochen hätte. In die Planungen wurde ich eingebunden. Ich habe dem Vorhaben zugestimmt, nachdem die Kollegen aus der Informationssicherheit das Verfahren als sicher eingestuft haben. Außerdem war für mich ausschlaggebend, dass es zunächst nur um Wetter- und Verkehrsmeldungen geht. Im Zusammenhang mit der Erzeugung der synthetischen Stimme der Sprecherin habe ich darauf hingewirkt, dass in dem Vertrag im Detail beschrieben wurde, wie mit der Aufzeichnung der Stimme verfahren wird. Außerdem wurde dem Vertrag eine ausführliche Datenschutzerklärung beigefügt.

2. Mobile Upload für das Mobile Reporting

Wie berichtet, findet seit Herbst 2018 beim rbb zusätzlich zu der herkömmlichen Produktionsform das ‚Mobile Reporting' statt. Reporter:innen drehen mit dem Smartphone und schneiden das Material anschließend mit dem Laptop selbst. Ich habe zuletzt in meinem 16. Tätigkeitsbericht darüber informiert (S. 67 ff.). Inzwischen hat es eine Erweiterung gegeben. Seit Frühjahr 2021 gibt es den sogenannten ‚Mobile Upload', ein Tool, mit dem fertige Beiträge oder Drehmaterial direkt in das Produktionssystem hochgeladen werden können – von überall dort, wo die Reporter:innen eine stabile Internet- oder WLAN-Verbindung haben. Zuvor war der Upload von Videodateien über die Austauschplattform ARD-ZDF-Box erfolgt. Das war insofern umständlich, als die Dateien zunächst von den Reporter:innen in die ARD-ZDF-Box hochgeladen und anschließend in den sogenannten Ingest-Centern aus der ARD-ZDF-Box wieder heruntergeladen und ins Produktionssystem eingespeist werden mussten. Der Mobile Upload wird von einem externen Dienstleister bereitgestellt. Da auch Nutzerdaten verarbeitet werden, habe ich auf den Abschluss einer Vereinbarung zur Auftragsverarbeitung mit dem Dienstleister hingewirkt und außerdem die Projektverantwortlichen bei der Formulierung der Datenschutzerklärung für die Reporter:innen unterstützt.

3. Neue Distributionsplattformen

Der rbb verbreitet seine Angebote zunehmend auch über Drittplattformen. Das ist vor dem Hintergrund des geänderten Nutzungsverhaltens der Rezipienten sicherlich geboten und entspricht auch seinem gesetzlichen Auftrag. Andererseits sind aus Datenschutzsicht viele Plattformen kritisch zu betrachten.

3.1. Sprachassistenten

Die gängigen Sprachassistenzdienste erfreuen sich trotz anfänglicher Skepsis zunehmender Beliebtheit, obwohl sie tief in die Privat- und Intimsphäre ihrer Nutzer:innen sowie unbeteiligter Dritter eindringen. Von der Möglichkeit, sich mit eigenen Anwendungen an die Sprachassistenzdienste anzubinden, hat dessen ungeachtet auch der rbb Gebrauch gemacht. Seit einiger Zeit sind Angebote aller rbb-Radiowellen auch über die Smartspeaker von Amazon

und Google abrufbar. Die Drittanbieter, wie z. B. der rbb, können über die Entwicklerplattform Berichte und Auswertungen über das Verhalten ihrer Nutzer:innen abrufen, bei Alexa sogenannte ‚Skill Metrics'. ‚Skill Metrics' wertet insbesondere die Anzahl der Nutzer:innen eines Skills, Informationen zum Ablauf einer Nutzer-Session sowie Kennzahlen zum Nutzerverhalten aus, z. B. regionale Verteilung der Nutzer:innen. Dieser Umstand führt dazu, dass die Drittanbieter – so auch der rbb- – gemeinsam mit den Sprachassistenzanbietern in einer gewissen datenschutzrechtlichen Verantwortung stehen. Auf die Notwendigkeit zum Abschluss eines Joint Controller-Vertrages habe ich die Abteilung Online-Koordination hingewiesen.

3.2. safespace auf TikTok

Den im letzten Jahr von Intendanz und Programmdirektion durchgeführten Ideenwettbewerb für ein crossmediales Angebot hat das Projekt ‚safespace' gewonnen, ein Angebot für Mädchen im Alter zwischen 14 und 16 Jahren mit dem Fokus auf die Themen Gesundheit und Schönheit. Es wird hauptsächlich auf TikTok verbreitet, einem internationalen Videoportal mit zusätzlichen Funktionen eines sozialen Netzwerks, das vom chinesischen Unternehmen ‚ByteDance' betrieben wird. Ich hatte im Vorfeld des Starts von ‚safespace' im Sommer 2020 Bedenken zur Verbreitung des Angebots über TikTok angemeldet. Die Plattform steht in der datenschutzrechtlichen Kritik, weil sie in größerem Stil Nutzerdaten verarbeitet und darüber nicht transparent informiert. Darüber hinaus unterdrückt sie Beiträge, die gegenüber dem chinesischen Regime politisch nicht opportun oder aus anderen Gründen unerwünscht sind. Die Nutzung von TikTok durch unter 13-Jährige ist laut deren Nutzungsbedingungen verboten. Für Jugendliche bis zur Vollendung des 18. Lebensjahres ist die Nutzung nur mit Zustimmung der Erziehungsberechtigten erlaubt. Alter und Zustimmung der Erziehungsberechtigten werden jedoch von TikTok nicht kontrolliert. Es gibt bei TikTok keine Möglichkeit des Monitorings und Kuratierens. Es kommt daher immer wieder vor, dass die Nutzer:innen in Kommentaren sensible personenbezogene Daten i. S. v. Art. 9 DSGVO über sich preisgeben. Ich hatte die Gelegenheit, meine Bedenken in einem längeren Gespräch mit dem Programmdirektor zu äußern. Er hat mir versichert, meine Hinweise sehr ernst zu nehmen. Deshalb werde der rbb zusätzlich zu den Gesundheitsthemen in ‚safespace' auch über den Schutz der Privatsphäre aufklären.

Herr Dr. Schulte-Kellinghaus hat mir angeboten, das Projekt gemeinsam nach zwölf Monaten zu evaluieren. Außerdem hat er meinen Vorschlag befürwortet, ein Gremium aus Datenschutz, Jugendschutz und Programm zu schaffen, das in regelmäßigen Abständen Drittplattformen als Distributionspartner für öffentlich-rechtliche Inhalte bewertet. Das Gremium wird sich in Kürze konstituieren.

3.3. Clubhouse

Clubhouse ist eine neue App für Audio-Talkshows. Über sie können sich App-Nutzer:innen Gespräche anhören und an Diskussionen teilnehmen. Es sind öffentliche Diskussionen, aber auch solche in geschlossenen Gruppen möglich. Ein/e Moderator:in spricht live über ein bestimmtes Thema und die Nutzer:innen können zuhörend teilnehmen. Sie sind zunächst stummgeschaltet, können aber einzeln von der Moderation zum Gespräch freigeschaltet werden. Clubhouse ist also eine Art ‚Live-Talkshow' ohne Kamera. Die RDSK hat sich mit der App im Februar 2021 beschäftigt und ist zu dem Ergebnis gekommen, dass die App aus mehreren Gründen datenschutzrechtlich sehr bedenklich ist: Ursprünglich erforderte sie den Zugriff auf alle auf dem Gerät der Nutzer:innen gespeicherten Kontakte, wenn diese selbst zu einer Gesprächsrunde einladen wollten. Außerdem fertigt Clubhouse Audiomitschnitte der Diskussionen, die nach eigenen Angaben ausschließlich zur Unterstützung der Untersuchung von Vorfällen aufgezeichnet werden. Die Aufzeichnungen werden ebenso wie die erhobenen Kontakt- und Accountinformationen der Nutzer:innen zumindest für eine gewisse Zeit in den USA gespeichert und verarbeitet sowie an verschiedene Unternehmen weitergegeben. Zusagen über ein der DSGVO vergleichbares angemessenes Niveau zum Schutz dieser Daten enthält die Datenschutzerklärung des Anbieters bislang nicht. In den Allgemeinen Geschäftsbedingungen und der unzulässigerweise nur in englischer Sprache formulierten Datenschutzerklärung wird die DSGVO bislang nicht erwähnt und eine Adresse für Datenschutzauskünfte in der EU nicht benannt. Die RDSK rät daher von der Nutzung der App bis auf weiteres dringend ab (s. „Entschließung der RDSK zu Clubhouse"; Stand Februar 2021, Anlage 4). Inzwischen ist die App überarbeitet worden. Mit der neuen Version müssen die Nutzer:innen, die Dritte zu einer Gesprächsrunde einladen wollen, der App nicht mehr Zugriff auf ihr gesamtes Adressbuch gewähren.

VI. Sonstiges

1. Datenschutz in der Abteilung Medienforschung

Ein intensiver Austausch fand im Berichtsjahr mit der Leitung der Abteilung Medienforschung statt. Obwohl in diesem Bereich regelmäßig sensible personenbezogene Daten verarbeitet werden, hatte die Abteilung in der Vergangenheit nur selten eine Beratung durch die Datenschutzbeauftragte in Anspruch genommen. Angesichts der Tatsache, dass die Medienforschung für die rbb-Angebote immer wichtiger wird, bin ich selbst auf diesen Bereich zugegangen. Wir haben gemeinsam die einzelnen Formate der Befragung der Rezipient:innen und die konkrete Vorgehensweise in den jeweiligen Fällen identifiziert. Dabei ging es zunächst um eine Klärung der Rolle der Agentur, mit der der rbb regelmäßig zusammenarbeitet, und um die Verteilung der datenschutzrechtlichen Verantwortlichkeiten.

Für den Bereich der Musikforschung haben wir herausgearbeitet, dass die komplette datenschutzrechtliche Verantwortlichkeit bei der Agentur verbleibt, mit der Folge, dass auch keine Vereinbarung zur Auftragsverarbeitung mit der Agentur abgeschlossen und das Verfahren auch nicht in das rbb-VVT aufgenommen werden muss. Ausschlaggebend für diese Einordnung war die Tatsache, dass der rbb eine komplette Studie bei der Agentur in Auftrag gibt und ein Ergebnis mit aggregierten Daten erhält. Mit personenbezogenen Daten kommt der rbb hier also gar nicht in Berührung. Zwar definiert er die Kategorie der Interview-Partner:innen und legt die Fragen fest, überlässt aber die Auswahl der konkret zu befragenden Personen und auch die Art der Befragung der Agentur.

Für die anderen Formate sind die Prüfungen noch nicht abgeschlossen.

2. Datenschutz in der Abteilung Marketing und PR

Eine intensive Zusammenarbeit fand im Berichtsjahr auch mit den Kolleginnen und Kollegen aus der Abteilung Marketing und PR statt.

2.1. Besucherdatenerfassung über EVENTIM.CheckIn

Um während der COVID-19-Pandemie überhaupt Veranstaltungen durchführen zu können, wäre in jedem Fall eine Besucherdatenerfassung zur Kontaktnachverfolgung erforderlich gewesen. Diesen neuen Aspekt musste die Abteilung Marketing und PR in ihre Planungen einbeziehen. Da der rbb bereits das ‚CTS-EVENTIM'-Ticketsystem für den Ticketverkauf für seine Veranstaltungen nutzt, lag es nahe, auch das erweiterte Angebote zur Besucherdatenerfassung von diesem Anbieter zu nutzen. ‚EVENTIM.CheckIn' bietet eine datenschutzkonforme Besuchererfassung. Sie umfasst die Möglichkeit, mit der ‚EVENTIM.CheckIn-Organiser'-App entsprechende Veranstaltungen ins System einzugeben und andererseits die Daten der Besucher:innen mit Hilfe der ‚EVENTIM'-App zu erfassen.

Die Prüfungen des Tools von Informationssicherheit und Datenschutz wurden abgeschlossen, eine Vereinbarung zur Auftragsverarbeitung mit dem Anbieter und eine Datenschutzerklärung vorbereitet. Leider kam das Tool mangels Durchführung entsprechender Veranstaltungen nicht zum Einsatz.

2.2. Einladungsmanagement mit Hilfe von MATE for Events

MATE for Events ist eine webbasierte Applikation für das Einladungsmanagement, den Newsletter-Versand sowie die Pflege von Verteilern. Die Applikation kam erstmalig bei der virtuellen Preview ‚Die ARKTIS' (ARD-Dokumentation) im November 2020 zum Einsatz.

Zuvor hatten der Informationssicherheitsbeauftragte und die Datenschutzbeauftragte das Betriebskonzept und den vom Betreiber zur Verfügung gestellten Vertrag zur Auftragsverarbeitung inkl. der Beschreibung der Technischen und Organisatorischen Maßnahmen (TOM) zur Datensicherheit und zum Datenschutz geprüft. Außerdem hat die Datenschutzbeauftragte bei der Formulierung der Datenschutzerklärung gegenüber den Eingeladenen unterstützt.

2.3. Besuchermanagementsystem mit Hilfe von Pretix

Für das Besuchermanagement einschließlich Time-Slot-Buchung und die Kontaktnachverfolgung im neuen ‚studioeins' von radioeins im Bikini-Berlin beabsichtigt die Abteilung Marketing und PR ab Juni 2021 die Ticketshop-Software Pretix einzusetzen. Der Informationssicherheitsbeauftragte hat das Betriebskonzept geprüft und den Einsatz von Pretix befürwortet. Ich habe Marketing und PR bei der Erstellung der weiteren datenschutzrechtlich relevanten Unterlagen unterstützt. Mit dem Betreiber von Pretix wurde die übliche Vereinbarung zur Auftragsverarbeitung abgeschlossen. Nachdem mir im Zusammenhang mit den Planungen für den Einsatz des Tools bekannt wurde, dass im Zusammenhang mit dem Besuchermanagement für studioeins auch die Agentur Brandyourlife für den rbb tätig wird, habe ich darauf gedrungen, auch mit diesem Dienstleister eine Vereinbarung zur Auftragsverarbeitung abzuschließen. Außerdem habe ich bei dem Entwurf der obligatorische Datenschutzerklärung für die Nutzer:innen des Systems unterstützt. Nachdem alle Dokumente in der finalen Fassung vorlagen, konnte das Verfahren in das VVT aufgenommen werden.

2.4. Einsatz von Microsoft Teams bei virtuellen Veranstaltungsformaten

Microsoft Teams bietet sich als Tool für unterschiedliche virtuelle Veranstaltungsformate an. Innerhalb einer Teams-Schalte lassen sich Menschen virtuell zusammenbringen und Inhalte teilen. Für zwei Veranstaltungsformate hat die Abteilung Marketing und PR Teams-Schalten gewählt: für die virtuellen Besucherführungen und den Girls Day.

2.4.1. Virtuelle Besucherführungen

Jährlich empfängt der rbb üblicherweise ca. 10.000 Besucher:innen, pandemiebedingt sind zurzeit aber keine Besucherführungen vor Ort möglich. Als Alternative hat Marketing und PR eine Teams-Videokonferenz hierfür entwickelt, in der ein/e Führer:in den virtuellen Besucher:innen mit Hilfe von vorproduzierten Videoclips und 360-Grad-Fotos den rbb und seine Arbeit vorstellt. Es erfolgt ein interaktiver Austausch mit dem Guide, der die Besucher:innen moderativ zu den einzelnen Stationen führt.

2.4.2. Girls‘ Day / Zukunftstag 2021

Pandemiebedingt fand der Girls‘ Day / Zukunftstag am 22.4.2021 virtuell statt. In neun parallelen Teams-Schalten wurden Mädchen und Jungen unterschiedliche Berufsbilder im rbb vorgestellt.

Ich habe die Verantwortlichen der Abteilung Marketing und PR bei dem Entwurf der Datenschutzerklärungen unterstützt. Die Besonderheit bestand darin, dass für die Teilnahme zusätzlich zu der Erklärung der minderjährigen Teilnehmer:innen auch die Einwilligungserklärung ihrer Eltern eingeholt werden musste. Das Verfahren wurde mit mir abgestimmt.

3. Digitale Sitzungen des Rundfunkrates

Am 18.2.2021 fand die erste Sitzung des rbb-Rundfunkrates per Microsoft Teams statt. In dieser Sitzung wurden auch Vorsitz und stellvertretender Vorsitz digital gewählt. Dafür wurde das Online-Wahlsystem des deutschen Anbieters ‚Polyas‘ angeschafft, das u. a. auch für die letzte CDU-Vorstandswahl eingesetzt wurde. Meine Kollegen aus der Informationssicherheit hatten das System im Vorfeld eingehend geprüft und konnten die Eignung bestätigen. Sie begleiteten den gesamten Planungsprozess bis hin zur Durchführung der Videokonferenz. Ich habe dafür gesorgt, dass mit dem Anbieter eine Vereinbarung zur Auftragsverarbeitung abgeschlossen wurde. An der Erarbeitung der den Rundfunkräten zusammen mit dem Link für die Teilnahme an der Videokonferenz versandten Datenschutzerklärungen für die Nutzung des Videokonferenzsystems und für den Einsatz des Online-Wahlsystems war ich beteiligt. Die im Zusammenhang mit der Durchführung der Videokonferenz anfallende Verarbeitung von personenbezogenen Daten wurde auf Art. 6 Abs. 1 c) DSGVO („Datenverarbeitung in Erfüllung einer rechtlichen Verpflichtung“) gestützt. Bei den Vorbereitungen war mir allerdings nicht bekannt und es fehlte daher auch in der Datenschutzerklärung der Hinweis darauf, dass der öffentliche Teil der virtuellen Sitzung des Rundfunkrates im Internet gestreamt würde. Das Streaming entsprach einer Maßgabe der Rechtsaufsicht. Diese hatte den Standpunkt vertreten, dass es aus Gründen der Rechtssicherheit, insbesondere um die Wirksamkeit von Beschlüssen zu gewährleisten, unabdingbar sei, den Grundsatz der Öffentlichkeit (§ 15 Abs. 6 rbb-StV) zu wahren.

Soweit der rbb-Rundfunkrat die Öffentlichkeit nicht durch Beschluss ausschließe, sei die Videokonferenz daher im elektronischen Übermittlungsweg (etwa als Livestream) zu übertragen. Es seien keine zwingenden Gründe ersichtlich, die dagegensprechen könnten, die Öffentlichkeit technisch mittels eines Livestreams herzustellen. Die der Maßgabe zugrundeliegende Rechtsauffassung wurde vom Justitiariat nicht in Zweifel gezogen. Auch die Datenschutzbeauftragte schloss sich dieser Sichtweise an, zumal die Rundfunkratsmitglieder im Rahmen der Rundfunkratssitzungen nicht als Privatpersonen von der Datenverarbeitung beim Livestreaming betroffen sind, sondern in ihrer Funktion als Rundfunkratsmitglieder und daher insgesamt weniger in ihren Persönlichkeitsrechten berührt sind. Die Rundfunkratsmitglieder wurden in der Einladung zur Sitzung, zu Beginn des Streamings und auch während der Sitzung von der Vorsitzenden wiederholt auf das Streaming hingewiesen. Am 15.4.2021 fand eine weitere Rundfunkratssitzung per Teams statt, die ebenfalls ins Internet gestreamt wurde. Die Datenschutzerklärung war im Vorfeld um den Hinweis auf das Streaming ergänzt worden. Auch in Zukunft sollen die Sitzungen wegen der Corona-bedingten Abstandsregelungen per Teams durchgeführt und ins Internet gestreamt werden.

D. Datenschutz beim Rundfunkbeitragseinzug

I. Allgemeines

Für den Einzug der Rundfunkbeiträge betreiben die Landesrundfunkanstalten auf der Grundlage von § 10 Abs. 7 RBStV im Rahmen einer nichtrechtsfähigen öffentlich-rechtlichen Verwaltungsgemeinschaft den Zentralen Beitragsservice (ZBS) in Köln. In der Verwaltungsvereinbarung Rundfunkbeitragseinzug von ARD, ZDF und DLR werden die Struktur des ZBS beschrieben und seine Aufgaben von denen der dezentralen Einheiten in den jeweiligen Landesrundfunkanstalten abgegrenzt.

Soweit der ZBS für den rbb tätig wird, gelten neben der DSGVO und den bereichsspezifischen Datenschutzregelungen des RBStV ergänzend die Regelungen des BlnDSG. Die betriebliche Datenschutzbeauftragte des rbb ist gemäß § 4 BlnDSG für die Überwachung der ordnungsgemäßen Datenverarbeitung beim Beitragseinzug zuständig. Zuständige Aufsichtsbehörde

gemäß Art. 51 DSGVO ist die Beauftragte für den Datenschutz des Landes Berlin (§ 38 Abs. 8 rbb-StV).

Unbeschadet der Zuständigkeit des/der nach Landesrecht für die jeweilige Landesrundfunkanstalt zuständigen Datenschutzbeauftragten ist beim ZBS gemäß § 11 Abs. 2 Satz 1 RBStV ein/e behördliche/r Datenschutzbeauftragte/r zu bestellen. Die/der behördliche Datenschutzbeauftragte arbeitet zur Gewährleistung des Datenschutzes mit dem/der nach Landesrecht für die jeweilige Rundfunkanstalt zuständigen Datenschutzbeauftragten zusammen und unterrichtet diese/n über Verstöße gegen Datenschutzvorschriften sowie über die dagegen getroffenen Maßnahmen. Im Übrigen gelten die für die bzw. den behördliche:n Datenschutzbeauftragte:n anwendbaren Bestimmungen der DSGVO entsprechend. Die behördliche Datenschutzbeauftragte und ihr Stellvertreter sind Mitglieder des AK DSB. Durch die Mitgliedschaft ist ein zeitnaher Austausch zu Datenschutzfragen im Zusammenhang mit dem Beitragseinzug gewährleistet. Um komplexere Themen besser vorbereiten zu können, hat der AK DSB einen Unterarbeitskreis ‚Beitragsdatenverarbeitung' gegründet, dessen Mitglied auch die Datenschutzbeauftragte des rbb ist.

II. Joint-Controller-Vertrag ZBS

Da die Rundfunkanstalten gemeinsam für die Datenverarbeitung durch den ZBS verantwortlich sind, mussten die Intendant:innen in Ergänzung zur Verwaltungsvereinbarung gemäß Art. 26 DSGVO noch eine Joint Controller-Vereinbarung über die konkrete Verteilung der datenschutzrechtlichen Verantwortlichkeiten abschließen. Dies ist inzwischen geschehen. Der AK DSB hatte den Entwurf dafür erarbeitet (s. 16. Tätigkeitsbericht, S. 80). Die wesentlichen Teile der Joint Controller-Vereinbarung sind auf der Webseite des ZBS veröffentlicht. Darüber hinaus wird Briefen zum Zweck der erstmaligen Kontaktaufnahme zu (potentiellen) Beitragsschuldner:innen eine entsprechende Information beigelegt.

III. Löschung von nicht mehr benötigten Beitragsschuldnerdaten

Die Umsetzung des im Vorjahresbericht erwähnten neuen Löschkonzepts (16. Tätigkeitsbericht, S. 79 f.) ist im Berichtsjahr erfolgreich vorangeschritten. Seit März 2020 wurden veraltete Stamm- und Korrespondenzanschriften, Befreiungsdaten, Mahnmaßnahmen und Buchungsbelege gelöscht. Die weiteren anstehenden Löschungen von Beitragsschuldnerdaten werden nun zunehmend komplexer, da sie auch Auswirkungen auf die Anzeigemasken in dem Beitragsverarbeitungssystem Rubin haben. Dennoch ist der Gesamtabschluss des Projekts für das Ende des zweiten Quartals 2021 geplant.

IV. Auskunftsersuchen und Eingaben

1. Bearbeitung durch den ZBS

Die Rundfunkanstalten haben die Bearbeitung von datenschutzrechtlichen Anfragen und sonstigem Routineschriftwechsel in Beitragsangelegenheiten dem ZBS übertragen. Die Bearbeitung von Geschäftsvorfällen mit grundsätzlichem Charakter und von individuellen Anfragen mit besonderer datenschutzrechtlicher Bedeutung hat er sich selbst vorbehalten. Im Berichtsjahr stand eine größere Änderung des Prozesses der Beauskunftung von Beitragsschuldnerdaten an, da der Auskunftsanspruch im RBStV mit Wirkung zum 1.6.2020 neu geregelt wurde (s. B. III. 1.2.). Wesentliche Änderung ist, dass Daten, die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen, vom datenschutzrechtlichen Auskunftsanspruch nicht umfasst sind.

Der ZBS hat diese gesetzliche Änderung dergestalt umgesetzt, dass das ursprünglich zweistufig ausgestaltete Verfahren auf eine einstufige Beantwortung der Auskunftsersuchen umgestellt wurde. Die ursprüngliche zweite Stufe der Auskunft, die vor allem historische Daten enthielt, ist entfallen. Das im Jahr 2020 noch praktizierte Verfahren sah folgendermaßen aus: In der ersten Stufe der Beauskunftung wurden im Wesentlichen die aktuellen Stammdaten zu einem Beitragskonto mitgeteilt. Zugleich wurde darauf hingewiesen, dass im Einzelfall weitere Daten

vorhanden sein können, die bei weiterer Nachfrage im Rahmen der Erstellung einer sogenannten erweiterten Auskunft zur Verfügung gestellt werden.

Seit Mitte Februar 2021 wird der neue Beauskunftungsbrief verwendet. Dieser Brief enthält nun sämtliche Datenkategorien, die gemäß der neuen Regelung im RBStV zu beauskunften sind. Neben der Möglichkeit, ein schriftliches Auskunftsersuchen an den ZBS zu richten, besteht die Möglichkeit, eine Datenschutzauskunft elektronisch zu beantragen. Für den Abruf über das ZBS-Onlineportal werden in diesem Fall vorab vom ZBS die Zugangsdaten per Post versandt.

Die Bearbeitung datenschutzrechtlicher Auskunftsersuchen und sonstiger Eingaben mit Datenschutzbezug (z. B. Antrag auf Löschung, Frage nach konkreter Herkunft von Anschriften) erfolgt vollständig durch ein gesondertes, speziell im Datenschutz geschultes Sachbearbeitungsteam.

Im Zeitraum 1.1.2020 bis 31.12.2020 hat der ZBS für den rbb insgesamt 2.787 einfache Datenauskünfte erteilt, davon 272 auf elektronischem Weg über das Onlineportal. Eine erweiterte Datenauskunft wurde nur in 26 Fällen beantragt und antragsgemäß erteilt. Im Vergleich dazu hatte der ZBS für den rbb im Jahr 2019 insgesamt 781 (davon 218 elektronisch) Auskunftsersuchen bearbeitet. Nur in 14 Fällen war die erweiterte Auskunft angefordert worden.

Die nachfolgende Übersicht liefert einen Überblick über die monatliche Entwicklung der datenschutzrechtlichen Eingaben bzw. der entsprechend ausgelösten Briefe beim ZBS für alle Landesrundfunkanstalten im Jahr 2020:

Jan.	**Feb.**	**März**	**April**	**Mai**	**Juni**	**Juli**	**Aug.**	**Sep.**	**Okt.**	**Nov.**	**Dez.**
21.129 (343)*	3.193 (254)	1.682 (237)	1.374 (266)	913 (259)	834 (236)	877 (277)	731 (236)	651 (241)	704 (287)	612 (265)	679 (256)

(* Bei den in Klammern angegebenen Werten handelt es sich um die elektronisch beantragten einfachen Datenauskünfte, bei denen vorab jeweils automatisiert ein Brief mit Zugangsdaten versandt wurde.)

Es wird deutlich, dass die Anzahl der Anträge auf Auskunft und Eingaben mit Datenschutzbezug vor allem zu Beginn des Jahres 2020 signifikant hoch war. Eine Ursache dafür ist höchstwahrscheinlich der Umstand, dass von Dezember 2019 bis ca. Ende Februar/Anfang März 2020 vor allem über die Internetseite ‚www.hallo-meinung.de' vehement zu Störungs- und Boykottaktionen gegen den Beitragseinzug und den öffentlich-rechtlichen Rundfunk aufgerufen wurde. Um die Menge der Anfragen bewältigen zu können, wurden vom ZBS Formulare zur Beantragung von Datenauskünften zum Ausdrucken und/oder Download zur Verfügung gestellt. Kommunikativ begleitet wurde dies im Rahmen einer umfassenden Kampagne in den sozialen Medien. Zum Jahresende konnte festgestellt werden, dass sich die Anzahl der Auskunftsersuchen wieder auf dem Niveau der Vorjahre eingependelt hatte.

2. Bearbeitung durch die Datenschutzbeauftragte des rbb

Bei der Datenschutzbeauftragten des rbb sind im Zeitraum 1.1.2020 bis 31.12.2020 insgesamt 13 Auskunftsersuchen und Eingaben zur Datenverarbeitung beim Beitragseinzug eingegangen. Im Jahr 2019 waren es noch 33 Auskunftsersuchen und Eingaben gewesen. Der Rückgang ist möglicherweise darauf zurückzuführen, dass die Informationen des ZBS auf der Internet-Seite ‚Rundfunkbeitrag.de' über die beim ZBS liegende Zuständigkeit für die Beantwortung von Auskunftsbegehren inzwischen von den Antragsteller:innen häufiger zur Kenntnis genommen werden. Ich habe die Vorgänge wie im Joint Controller-Vertrag festgelegt, direkt an den ZBS zur Bearbeitung abgegeben.

V. Beschwerden zur Datenverarbeitung beim Beitragseinzug

Über die zuständige Aufsichtsbehörde, die Berliner Beauftragte für Datenschutz (BlnDSB), erreichten die rbb-Datenschutzbeauftragte insgesamt sechzehn Beschwerden.

In mehreren Fällen ging es um den Umfang der durch den ZBS erteilten Auskunft. Viele Beschwerden bezogen sich auch auf die Sachbearbeitung durch den ZBS. Zu sämtlichen

Beschwerden wurde in Abstimmung mit der Datenschutzbeauftragten des ZBS ausführlich gegenüber der Berliner Beauftragten für Datenschutz Stellung genommen. Dabei wurde darauf verzichtet, die Beantwortung von Fragen zur Sachbearbeitung auszusparen, wenngleich diese Themen nicht in die Zuständigkeit der Datenschutzbeauftragten fallen.

In den meisten Fällen endete das Beschwerdeverfahren mit der Stellungnahme der rbb-Datenschutzbeauftragten. In einem Fall kam es zu einer Verwarnung gemäß Art. 58 Abs. 2 b) DSGVO durch die Berliner Beauftragte für Datenschutz. Der Verwarnung lag folgender Sachverhalt zugrunde:

Im Zusammenhang mit einem gegenüber dem ZBS im Jahr 2018 geltend gemachten Auskunftsersuchen hatte der Petent als Identitätsnachweis freiwillig eine Kopie seines Personalausweises übersandt. Er hatte darum gebeten, die Kopie unverzüglich nach erfolgter Identitätsprüfung zu vernichten. Dieser Bitte war der ZBS zunächst nicht nachgekommen. Nach dem Einscannen der Eingangspost war die Kopie im Beitragskonto des Petenten verblieben, da der ZBS der Meinung war, die Kopie als Bestandteil der Korrespondenz archivieren zu dürfen und ihm zum damaligen Zeitpunkt das Herauslöschen einzelner Seiten aus dem Beitragskonto auch gar nicht möglich war. Nachdem der ZBS im Frühherbst 2020 eine technische Lösung zur manuellen Herauslösung einzelner Dokumente aus dem Beitragskonto entwickelt hatte, teilte ich dies der Behörde mit. Außerdem habe ich die Löschung der Kopie des Personalausweises und eine entsprechende Information an den Petenten veranlasst. Die Berliner Datenschutzbeauftragte ließ offen, ob es überhaupt rechtens sei, die im Zusammenhang mit einem Auskunftsersuchen eingereichte Ausweiskopie im Beitragskonto des Petenten zu speichern. Wenn überhaupt, sei dies aber jedenfalls nur für einen sehr kurzen Zeitraum – bis zum Ende der Identitätsprüfung – zulässig. Die Speicherung der Kopie über diesen Zeitraum hinaus wertet die Berliner Datenschutzbeauftragte als einen Verstoß gegen die DSGVO.

Wie der rbb schon einmal erfahren musste (s. 16. Tätigkeitsbericht, S. 85 f.), sieht sich die BlnDSB in jedem Falle eines Verstoßes gegen die DSGVO – unabhängig von den Umständen und der Schwere – veranlasst, auf diesen Verstoß mit einer Abhilfemaßnahme zu reagieren. Dabei ist die Verwarnung das mildeste Mittel. Angesichts der Tatsache, dass der ZBS inzwischen eine technische Lösung zum manuellen Löschen einzelner Dokumente aus dem

Beitragskonto entwickelt hat und somit vergleichbare Probleme nicht mehr auftreten dürften, ist der rbb auch dieser Verwarnung nicht entgegengetreten, sondern hat die Sache auf sich beruhen lassen.

E. Datenschutz im Informationsverarbeitungszentrum (IVZ)

I. Allgemeines

Das Informationsverarbeitungszentrum (IVZ) ist eine Kooperation aller ARD-Rundfunkanstalten sowie von Deutschlandradio und Deutscher Welle in Form einer öffentlich-rechtlichen nichtrechtsfähigen Verwaltungsgemeinschaft. Das IVZ ist beim rbb angesiedelt und auch an den Standorten anderer Landesrundfunkanstalten aktiv. Die Landesrundfunkanstalten kooperieren über das IVZ rund um die SAP-Anwendungen sowie bezüglich der Archiv- und Produktionssysteme.

II. Joint-Controller-Vertrag

Die inhaltliche und rechtliche Grundlage der IVZ-Kooperation bildet die IVZ-Verwaltungsvereinbarung. In Ergänzung dazu haben die Intendantinnen und Intendanten am 22.9.2020 eine Vereinbarung zur gemeinsamen Verantwortlichkeit bei der Verarbeitung von personenbezogenen Daten beim IVZ (Joint-Controller-Vertrag gemäß Art. 26 DSGVO) abgeschlossen. Darin sind u. a. die Zwecke und Mittel der Datenverarbeitung, die Erfüllung der datenschutzrechtlichen Verpflichtungen, die technischen und organisatorischen Maßnahmen zur Datensicherheit und die Informationspflichten des IVZ geregelt. Für die Kontrolle des Datenschutzes sind alle Rundfunkdatenschutzbeauftragten der am IVZ beteiligten Rundfunkanstalten zuständig. Als Datenschutzbeauftragte der Sitzanstalt ist die Datenschutzbeauftragte des rbb federführend für das IVZ zuständig. Zusätzlich hat das IVZ laut Joint-Controller-Vertrag einen eigenen Datenschutzbeauftragten zu bestellen, der die anfallenden Aufgaben nach Art. 39 DSGVO wahrnimmt. Der betriebliche Datenschutzbeauftragte des IVZ arbeitet mit den

Datenschutzbeauftragten der für die jeweilige Datenverarbeitung zuständigen Rundfunkanstalten kooperativ zusammen. Er erstellt einen jährlichen Tätigkeitsbericht.

III. IVZ-Jahrestreffen

Einmal jährlich findet beim IVZ das ‚Jahrestreffen IT-Sicherheit und Datenschutz' statt. Auf diesem Treffen informiert der Geschäftsführer u. a. über datenschutzrelevante Themen des zurückliegenden Jahres. Das letzte Jahrestreffen fand am 1.12.2020 per Videokonferenz statt. In dieser Videokonferenz hat sich der zum 1.11.2020 bestellte externe betriebliche Datenschutzbeauftragte Herr Dilyan Ivanov vorgestellt. Weitere Schwerpunkte der Videokonferenz waren das bestandene Re-Zertifizierungs-Audit ISO 27001 des IVZ, der Stand der Konsolidierung der Rechenzentren, der Stand des Projektes ‚(D)einSAP' und die Rolle des IVZ sowie die sogenannte ‚Liste der Risiken' in der Informationssicherheit. Diese Liste legt das IVZ regelmäßig dem Lenkungsausschuss vor. Bei neuen Risiken halten die Datenschutzbeauftragten ihre Einbeziehung für erforderlich. Das Ziel ist, vor einer eventuell rein betriebswirtschaftlichen Einschätzung durch die beauftragenden IT-Leiter eine Abstimmung mit den Datenschutzbeauftragten sicherzustellen. Der betriebliche Datenschutzbeauftragte des IVZ soll neu erkannte Risiken zukünftig bereits im Quartalsbericht mit einer Einschätzung versehen. Eine eventuell notwendige Folgebearbeitung im AK DSB wird bis auf weiteres durch die Datenschutzbeauftragte des rbb veranlasst.

F. Dokumentenarchiv ARD-Generalsekretariat (ARD-GS)

Das ARD-Generalsekretariat führt das digitale Schriftgutarchiv der ARD (§ 3 Abs. 3 Verwaltungsvereinbarung ARD-GS) in einem eigenen passwortgeschützten Bereich im System PAN. Im Rahmen der ARD-Strukturreform wird dieses System in den Media Data Hub (MDH) überführt. Der Datenbestand von zurzeit ca. 450.000 Dokumenten kann dort allerdings nicht abgebildet werden, so dass eine eigene Lösung ausgeschrieben wurde. Für den Datenbestand wurde im März 2020 nach dem ARD-Standardverfahren zuerst eine Schutzbedarfsfeststellung

durch den Informationssicherheitsbeauftragten durchgeführt. Im Ergebnis wurde ein hoher Schutzbedarf festgestellt. Das ARD-Generalsekretariat hat sich für die Lösung eines deutschen Anbieters entschieden, die auf dem rbb eigenen SharePoint im rbb Microsoft-365-Tennant in der Cloud aufsetzt. Der Dienstleister stellt dafür lediglich eine Konfiguration (insbesondere Oberfläche und Datenfelder für die Dokumentenablage) zur Verfügung. Die Daten sollen durch besondere Verschlüsselung geschützt werden. Der Schlüssel bleibt beim ARD-GS. Microsoft erhält keinen Zugriff auf den Schlüssel.

Der rbb-Informationssicherheitsbeauftragte hat keine Bedenken gegen den Einsatz des in Aussicht genommenen Systems. Die Datenschutzbeauftragte war an dem Ausschreibungsverfahren nicht beteiligt. Sie hält die Einschätzung des Informationssicherheitsbeauftragten in Bezug auf die Vertraulichkeit für plausibel, wonach die Daten durch das besondere Verschlüsselungssystem sicher sind. Allerdings hat sie die Frage aufgeworfen, ob den hohen Anforderungen an die Verfügbarkeit der Dokumente durch Ablage in der Microsoft-Cloud hinreichend Rechnung getragen ist. Sie hat auf die Notwendigkeit eines Backups hingewiesen. Die weiteren Planungsschritte bleiben abzuwarten.

G. Sonstige Eingaben und Beschwerden

Neben den unter D. IV. erwähnten Eingaben und Beschwerden zur Beitragsdatenverarbeitung haben die Datenschutzbeauftragte im Jahr 2020 16 sonstige Eingaben und Beschwerden erreicht (Zum Vergleich: Im Jahr 2019 waren 21 sonstige Eingaben und Beschwerden eingegangen). Auf nicht spezifische Auskunftsersuchen und Löschbegehren habe ich zunächst mit einem standardisierten Zwischenbescheid reagiert und um eine Spezifikation des Begehrens gebeten. Ziel dieses zweistufigen Verfahrens ist es, eine gezielte und datensparsame Abfrage innerhalb des rbb zu ermöglichen. Auf den Zwischenbescheid haben lediglich vier Antragsteller:innen nochmals reagiert. Davon begehrte ein Antragsteller eine Beauskunftung ausschließlich in Beitragsangelegenheiten. Dieses Verfahren konnte an den ZBS abgegeben werden. Drei

der Antragsteller:innen bestanden auf der Prüfung aller Bereiche im rbb (einschließlich ZBS), die ich daraufhin veranlasst habe. Den auf die Beitragsdatenverarbeitung bezogenen Teil des Ersuchens habe ich dabei ebenfalls an den ZBS abgegeben.

Aus dem Kreis der rbb-Beschäftigten ging eine Frage zur Zulässigkeit des Messengers WhatsApp auf Diensthandys ein. WhatsApp ist seit 2014 Teil der Facebook Inc. Benutzer:innen können über WhatsApp Textnachrichten, Bild-, Video- und Ton-Dateien sowie Standortinformationen, Dokumente und Kontaktdaten zwischen zwei Personen und auch zwischen Gruppen austauschen. Die Installation von WhatsApp auf Diensthandys ist insbesondere wegen der Möglichkeit des Auslesens von Adressen und der Weitergabe von personenbezogenen Daten an Facebook durch WhatsApp kritisch zu sehen. Andererseits macht es die journalistische Arbeit mitunter notwendig, auch über WhatsApp zu kommunizieren. Außerdem dürfen Dienstgeräte auch privat genutzt werden, wenn dies mit beantragt wurde. Gerade im Privatbereich ist WhatsApp sehr verbreitet, so dass ein Verbot problematisch wäre. Ich habe dem Fragesteller geantwortet, dass der rbb den von ihm angesprochenen Problemen so weit wie möglich Rechnung getragen hat. Alle dienstlichen Kontakte sind seit der Umstellung auf Microsoft 365 innerhalb der Office-365-Apps gekapselt. Das rbb-Adressbuch wird nicht in die Kontaktliste der Dienstgeräte synchronisiert. WhatsApp erhält somit keinen Zugriff auf dienstliche Kontakte. Eine Ausnahme bilden Kontakte, die die Nutzer:innen manuell im Adressbuch des Telefons anlegen. Deshalb gilt, dass dienstliche Kontakte in das dienstliche Adressbuch in Outlook gehören.

Zwei Eingaben bezogen sich auf den von freien Mitarbeiter:innen auszufüllenden Fragebogen als Voraussetzung zur Auszahlung von Honoraren. Der Inhalt des Fragebogens ist mit der Datenschutzbeauftragten abgestimmt und enthält ausschließlich die für die Bearbeitung der Honorare notwendigen Fragen. Liegt zwischen zwei honorarpflichtigen Tätigkeiten für den rbb ein Zeitraum von mehreren Jahren, ist das erneute Ausfüllen des Fragebogens erforderlich, da sich persönliche Daten, wie z. B. die Bankverbindung, geändert haben könnten.

Eine Anfrage zum Umgang mit freiwillig gegenüber der HA Personal angegebenen privaten Telefonnummern veranlasste mich dazu klarzustellen, dass diese nicht ohne Zustimmung der Betroffenen an die jeweiligen Fachbereiche weitergegeben werden dürfen.

Im Zusammenhang mit der Umstellung von dem schriftlichen auf den elektronischen Nachweis der Gehaltsabrechnungen im SAP-System xSS (s. C. IV. 2.) erreichte mich die Zuschrift einer Mitarbeiterin, die es mit Blick auf mögliche Hackerangriffe kritisch sah, dass auf jeder Abrechnung die Bankverbindung vollständig angegeben ist. Nach Rücksprache mit der HA Personal und den Kollegen von der Informationssicherheit teilte ich ihr mit, dass die Bankverbindung schon vor Einführung des elektronischen Gehaltsnachweises aus Transparenzgründen auf den Entgeltbescheinigungen aufgedruckt war. Für die Beschäftigten ist damit erkennbar, auf welches Konto das Gehalt überwiesen wird und auch welches Konto der rbb in den Stammdaten des Beschäftigten im SAP-System speichert. Zugriff auf die elektronische Gehaltsabrechnung und die darin enthaltenen personenbezogenen Daten in xSS haben nur die Mitarbeiter:innen persönlich. Durch die Follow-Me-Funktion (Druckauftrag wird durch Aktivierung durch den Hausausweis am Etagendrucker ausgelöst) ist sichergestellt, dass nur der/die jeweilige Mitarbeiter:in Einblick in die Ausdrucke erhält. Ein Zugriff auf xSS von außen ist ausschließlich über eine verschlüsselte Verbindung möglich. Dabei erfolgt der Zugriff auf einen virtuellen rbb-Client. Über das Internet wird nur die Anzeige übertragen und die Verbindung ist dabei verschlüsselt. Ein Datenabfluss ist also auf dem Weg vom rbb zu den Mitarbeiter:innen nicht möglich. Die Abrechnung kann auf diesem Weg nicht aus dem rbb heraus geladen werden – ein Download landet auf dem virtuellen rbb-Client im rbb. Auch ein Ausdruck über private Hardware ist nicht möglich.

Eine Kollegin bat mich um eine Bestätigung, dass die mit dem Umfragetool ‚Lama Poll' durchgeführte Mitarbeiterumfrage zum rbb-Leitbild wirklich anonym sei. Dies konnte ich bestätigen, da bei der Nutzung des Tools die Zuordnung der Antworten zu einer Person technisch ausgeschlossen ist (zu Datenschutz und Datensicherheit im Zusammenhang mit der Nutzung von ‚LamaPoll' s. 16. Tätigkeitsbericht, S. 61 ff).

Zwei externe Eingaben bezogen sich auf die Einwilligungsbedürftigkeit von Cookies nach dem Urteil des EuGH und BGH (s. dazu B. II. 2.2.). Ein weiterer Beschwerdeführer wandte sich gegen die Corona-bedingte Praxis des rbb, Bewerberinterviews per Videokonferenz zu führen. Im Speziellen lehnte er die Nutzung von Microsoft Teams ab. Der Beschwerdeführer hatte sich auf eine Stelle des rbb beworben, es jedoch abgelehnt, das Vorstellungsgespräch per

Videokonferenz zu führen. Daraufhin hatte ihm der rbb mitgeteilt, dass er im weiteren Verlauf des Ausschreibungsverfahrens nicht mehr berücksichtigt werden könne. Der Beschwerdeführer sah darin einen unzulässigen Eingriff in seine Privatsphäre. Nach Rücksprache mit der HA Personal teilte ich dem Beschwerdeführer mit, dass der rbb aufgrund der Corona-bedingten Vorgaben zur Kontaktbeschränkung Ende März 2020 kurzfristig gezwungen war, eine Alternative zu persönlichen Vorstellungsgesprächen zu entwickeln, um die Bewerbungsprozesse weiterhin fortführen zu können. Bei den Überlegungen schied das klassische Telefonat von vornherein mangels hinreichender Aussagekraft aus. Die Video-Telefonie bietet demgegenüber eine weitaus bessere Simulation eines ‚echten' Bewerbungsgesprächs, da sich die Gesprächsteilnehmer:innen tatsächlich gegenübersitzen und so mehr Eindrücke voneinander entstehen können. Diese Eindrücke wie Mimik, Gestik und die Reaktion auf Fragen, ist für beide Seiten mitentscheidendes Kriterium für den Fortlauf des Bewerbungsprozesses.

Der rbb hat sich bei der Auswahl eines Video-Telefonsystems für Microsoft Teams entschieden. Der Sitz von Microsoft befindet sich zwar in den USA und damit außerhalb des Geltungsbereichs der DSGVO, jedoch hat der rbb mit Microsoft die Standardvertragsklauseln vertraglich vereinbart, die gewährleisten, dass Microsoft die Vorgaben der DSGVO beachtet. Darüber hinaus ist durch den Abschluss eines Auftragsverarbeitungsvertrages zwischen dem rbb und Microsoft sichergestellt, dass das Unternehmen die Datenverarbeitung nur nach Weisung des rbb vornimmt.

Ein Verstoß gegen das allgemeine Persönlichkeitsrecht der Bewerber:innen durch den Einsatz von Videokonferenzsystemen bei Vorstellungsgesprächen liegt m. E. nicht vor. Rechtsgrundlage ist während der Corona-bedingten Kontaktbeschränkungen § 36 rbb-Staatsvertrag i. V. m. § 18 Berliner Datenschutzgesetz i. V. m. § 26 Bundesdatenschutzgesetz. Das Verfahren ist insgesamt datenschutzkonform gestaltet. Die Bewerber:innen erhalten mit der Einladung zum Gespräch per Videokonferenz eine Datenschutzerklärung. Eine Aufzeichnung der Gespräche findet nicht statt. Sollte der rbb nach dem Ende der Corona-bedingten Kontaktbeschränkungen auch weiterhin Bewerbungsgespräche per Videokonferenz führen, so wäre dies nur mit der ausdrücklichen Einwilligung der Bewerber:innen möglich.

In Kopie erreichte mich die Mail eines Hörers von rbb 88.8, der sich an die Berliner Datenschutzbeauftragte mit der dringenden Bitte gewandt hat, die Nutzung von WhatsApp im öffentlich-rechtlichen Rundfunk zu prüfen und möglichst zügig zu unterbinden. Der Hintergrund der Beschwerde war die MA-Kampagne ‚Everybody hörts', bei der rbb 88.8 WhatsApp als Rückkanal für die Hörer:innen genutzt hat. Bei der Kampagne handelte es sich um ein Ratespiel, bei dem Musiktitel umschrieben wurden. Die Hörer:innen wurden aufgefordert, ihre Lösung einschließlich Begründung an die Redaktion per WhatsApp zu schicken. Wahlweise nutzte 88.8 die ermittelte Nummer auch für einen Rückruf, falls der Redaktion ein Beitrag für ein Live-Telefonat geeigneter erschien.

Ich habe dem Beschwerdeführer mitgeteilt, dass die Berliner Beauftragte für Datenschutz und Informationsfreiheit nicht zuständig für die Frage ist, ob und in welcher Form der rbb in seinen Programmen bzw. in seinen Online-Angeboten auf Soziale Netzwerke zugreift. Nach Rücksprache mit dem Leiter von rbb 88.8 habe ich außerdem mitgeteilt, dass ich die Kritik an WhatsApp grundsätzlich teile. Ich habe aber auch die Motive der Redaktion erläutert, diesen Rückkanal zu nutzen. Er werde von den meisten Hörer:innen akzeptiert und deswegen auch ohne Vorbehalte genutzt. Außerdem werden zusätzlich zur Nutzung von WhatsApp stets auch andere Möglichkeiten eines Rückkanals angeboten. Ich habe die Beschwerde zum Anlass genommen, die Programmdirektion daran zu erinnern, die Entwicklung eigener datenschutzkonformer technischer Lösungen für einen Rückkanal für die Hörer:innen zu beschleunigen.

Über Umwege erreichte mich eine Datenschutzbeschwerde zu einem Videospiel mit dem Titel ‚Reichstagsdefender', das der rbb in das ARD-/ZDF-Jugendangebot ‚FUNK' eingebracht hat und das nach wie vor im Internet abrufbar ist. Das Videospiel ist im Auftrag des rbb von einer Produktionsfirma entwickelt worden, die auch das Hosting übernimmt. Die Beschwerdeführerin befürchtete einen Zusammenhang zwischen ihrer Teilnahme an dem Spiel und telefonischen Werbeanrufen, die sie auffallend häufig danach erreichten. FUNK konnte nachweisen, dass keine Kausalität zwischen der Teilnahme an dem Spiel und den Werbeanrufen bestand. Die dahingehende Beantwortung der Beschwerde übernahm der nach dem Federführerprinzip zuständige Rundfunkdatenschutzbeauftragte des SWR. Durch meine Befassung mit dem Sachverhalt hatte ich allerdings entdeckt, dass in der Datenschutzerklärung zum Online-Spiel

nicht ‚FUNK' bzw. ARD und ZDF als datenschutzrechtliche Verantwortliche genannt waren, sondern die mit dem Hosting betraute Produktionsfirma. Außerdem sah die Erklärung den Einsatz von Analysetools vor, die im öffentlich-rechtlichen Rundfunk nicht eingesetzt werden (u. a. Google Analytics). Ich habe mich daraufhin an den im rbb zuständigen Redakteur für ‚FUNK' gewandt und darauf hingewirkt, dass die Datenschutzerklärung korrigiert wurde.

H. Informationsmaßnahmen

Neben den in diesem Bericht an anderen Stellen bereits erwähnten spezifischen Informationsmaßnahmen haben die Datenschutzbeauftragte und ihr Stellvertreter im Berichtszeitraum folgende Datenschutzschulungen durchgeführt:

Gemeinsam mit dem Informationssicherheitsbeauftragten hat die Datenschutzbeauftragte am 11.2.2021 eine für die Führungskräfte obligatorische Schulung zu Datenschutz und Informationssicherheit durchgeführt. Am 16.10.2020 hat die Datenschutzbeauftragte zusammen mit dem stellvertretenden Informationssicherheitsbeauftragten die jährliche Datenschutzschulung für neue Auszubildende durchgeführt.

Der stellvertretende Datenschutzbeauftragte hat am 11.11.2020 und 17.2.2021 gemeinsam mit Mitarbeiterinnen und Mitarbeitern der HA MIT die für SAP-Nutzer:innen obligatorische Datenschutzschulung durchgeführt.

Die HA Personal hat im Sommer 2019 die electronic media school (ems) damit beauftragt, ein E-Learning-Angebot zum Datenschutz im rbb zu erstellen (s. 16. Tätigkeitsbericht, S. 19). Träger der ems sind die Medienanstalt Berlin-Brandenburg (mabb) und der rbb. Als Arbeitsgrundlage hatte die Datenschutzbeauftragte der ems ihr eigenes umfangreiches Schulungsmaterial zur Verfügung gestellt und ergänzende mündliche Erläuterungen gegeben. Nachdem die ems auf dieser Grundlage lange kein Konzept geliefert hatte, nahm die HA Personal die Sache selbst in die Hand und erstellte in Zusammenarbeit mit den Kollegen aus der Informationssicherheit, meinem Stellvertreter und mir den kompletten Inhalt der Schulung. Im Frühjahr 2021 konnte

die ems die technische Umsetzung fertigstellen. Nach Abstimmung mit dem Personalrat kann das E-Learning Datenschutz nun endlich im Frühsommer 2021 starten. Alle neuen Mitarbeiter:innen werden zukünftig im Onboarding-Prozess, also bei der Einstellung, aufgefordert, die Schulung zu durchlaufen und nach bestandenem Test das erworbene Zertifikat an die HA Personal zu schicken. Außerdem müssen alle Mitarbeiter:innen des rbb die Schulung einschließlich Test absolvieren, deren letzte Datenschutzschulung vor Sommer 2018 (also vor Wirksamwerden der DSGVO) stattgefunden hat.

I. Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und DLR

Die Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten arbeiten im Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und DLR (AK DSB) zusammen. Ein wesentliches Ziel ist es dabei, den Datenschutz bei den gemeinsamen Programmangeboten und beim Beitragseinzug nach möglichst einheitlichen Kriterien und Standards sicherzustellen. Zudem setzt das bei Beschaffungen im öffentlich-rechtlichen Rundfunk immer häufiger durchgeführte Leadbuyer-Verfahren, bei dem eine Rundfunkanstalt federführend Verhandlungen auch für alle anderen Rundfunkanstalten führt, voraus, dass im Datenschutz alle Rundfunkanstalten das gleiche Verständnis – beispielsweise hinsichtlich des Schutzbedarfs der mit einem System zu verarbeitenden Daten – haben.

Im Berichtszeitraum hat der AK DSB unter dem Vorsitz des Datenschutzbeauftragten des NDR, Herrn Dr. Heiko Neuhoff, am 23.4.2020 und am 19./20.11.2020 per Videokonferenz getagt.

Schwerpunkte der Konferenz am 23.4.2020, an der zeitweilig der Gesamtprojekt-Manager von (D)ein SAP, Herr Dr. Backhaus, und die Koordinatorin für Rechtsfragen, Monika Wolf, teilgenommen haben, bildeten u. a.

- Einzelfragen im Zusammenhang mit dem Projekt (D)ein SAP zur SAP-Harmonisierung innerhalb der ARD,
- der Einsatz von Videokonferenzsystemen,

- datenschutzrechtliche Einzelfragen im Zusammenhang mit dem Beitragseinzug,
- Joint-Controller-Verträge für ZBS, IVZ und ARD-Sternpunkt.

Am 19./20.11.2020 standen u. a. folgende Themen auf der Agenda:

- Datenschutzrechtliche Einzelfragen im Zusammenhang mit dem Beitragseinzug,
- Einzelfragen im Zusammenhang mit dem Projekt (D)ein SAP (in Anwesenheit von Herrn Dr. Backhaus und Frau Wolf),
- Empfehlungen des EDSA zum ‚Schrems II'-Urteil des EuGH,
- Konsequenzen für die Rundfunkanstalten aus dem Brexit,
- Verabschiedung eines gemeinsam mit der CC ISec erarbeiteten Daten-Klassifizierungskonzepts,
- Cloud Telefonie,
- Projekt SIEM/SOC.

Herr Dr. Heiko Neuhoff wurde für das Jahr 2021 im Amt des Vorsitzenden des AK DSB bestätigt. Herr Stephan Schwarze, Rundfunkdatenschutzbeauftragter des MDR, wurde für das Jahr 2021 im Amt des stellvertretenden Vorsitzenden des AK DSB bestätigt. Für das Jahr 2022 haben die Mitglieder des AK DSB den Datenschutzbeauftragten des BR, Herrn Axel Schneider, zum Vorsitzenden und den Datenschutzbeauftragten des ZDF, Herrn Gerold Plachky, zu seinem Stellvertreter gewählt. Im Jahr 2023 wird Herr Plachky den Vorsitz und Herr Schneider die Stellvertretung übernehmen.

J. Rundfunkdatenschutzkonferenz

Wie berichtet (16.Tätigkeitsbericht, S. 92ff.) hat sich im Mai 2019 die Rundfunkdatenschutzkonferenz (RDSK) konstituiert. Mitglieder sind die für die Datenschutzaufsicht zuständigen

Rundfunkdatenschutzbeauftragten von BR, DLR, WDR, SR, ZDF, MDR, NDR und SWR. Die Datenschutzbeauftragten des HR, RB, rbb und DW sind als Aufsichtsbehörden für den journalistisch-redaktionellen Teil der Datenverarbeitung der jeweiligen Rundfunkanstalten Mitglieder der RDSK.

Zu den Aufgaben der RDSK gehört es insbesondere, die Aufgaben nach Art. 57 DSGVO und die Befugnisse nach Art. 58 DSGVO zu koordinieren und gemeinsame Positionen zu wichtigen datenschutzrechtlichen Fragen zu entwickeln. Im Verhältnis zum AK DSB, der sich auf den operativen Bereich konzentriert, beschäftigt sich die RDSK mit Grundsatzfragen. Sie kann bei Fragen nach der datenschutzrechtlichen Zulässigkeit vorab konsultiert oder um eine generelle Einschätzung gebeten werden. Eine Geschäftsordnung regelt die wichtigsten Fragen zur Verständigung in Form von Beschlüssen, Entschließungen oder Empfehlungen.

In zwei Verwaltungsvereinbarungen vom 29.7.2020 haben die Mitglieder die Federführungen und die Abstimmungsprozesse für die Aufsicht über die rechtlich unselbstständigen Gemeinschaftseinrichtungen und über Gemeinschaftsunternehmen festgelegt. Die rbb-Datenschutzbeauftragte nimmt demnach die Datenschutzaufsicht federführend über die folgenden Gemeinschaftseinrichtungen wahr:

- ARD-Generalsekretariat
- ARD-Hauptstadtstudio
- ARD Play-Out-Center
- ARD Text
- Informationsverarbeitungszentrum (IVZ)

Da die rbb-Datenschutzbeauftragte laut rbb-Staatsvertrag wie auch die Datenschutzbeauftragten von hr, RB und DW keine Zuständigkeit für die Kontrolle des Datenschutzes in den Beteiligungsunternehmen des rbb hat, hat sie an der Verwaltungsvereinbarung für die Aufsicht über Gemeinschaftsunternehmen nicht mitgewirkt. Auf der neuen Internetseite der RDSK (https://www.rundfunkdatenschutzkonferenz.de/) werden jetzt deren Entschließungen, datenschutzrechtliche Eckpunkte und Positionspapiere veröffentlicht.

Folgende Videokonferenzen der RDSK fanden unter dem Vorsitz von Herrn Dr. Neuhoff im Berichtszeitraum statt:

Videokonferenz am 29.7.2020 mit folgenden Schwerpunktthemen:

- Urteil des BGH vom 28.5.2020 zum Einsatz von Cookies
- Konsequenzen für die Aufsichtsbehörden aus dem EuGH-Urteil zum Privacy-Shield (‚Schrems II')
- Verwaltungsvereinbarungen zur Wahrnehmung der Datenschutzaufsicht über Gemeinschaftseinrichtungen der Rundfunkanstalten und zur Wahrnehmung der Datenschutzaufsicht über Gemeinschaftsunternehmen der Rundfunkanstalten

Videokonferenz am 10.12.2020 mit dem Schwerpunktthema:

- Organisatorische Fragen, u. a. Homepage und Logo sowie Teilnahme an den DSK-Arbeitskreisen

Zum Vorsitzenden der RDSK für die Jahre 2021 und 2022 wurde der Rundfunkdatenschutzbeauftragte von BR, DLR, WDR, SR und ZDF, Herr Dr. Binder, gewählt. Für den gleichen Zeitraum wurde die rbb-Datenschutzbeauftragte zu seiner Stellvertreterin gewählt.

K. Zusammenarbeit der datenschutzrechtlichen Aufsichtsbehörden nach der DSGVO

Entsprechend der föderalen staatlichen Gliederung in Deutschland gibt es neben dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) jeweils unabhängige Aufsichtsbehörden in den einzelnen Bundesländern. Der BfDI ist zuständig für öffentliche Stellen des Bundes und Unternehmen, die Post- bzw. Telekommunikationsdienstleistungen erbringen. Die Zuständigkeit der Aufsichtsbehörden der Länder erstreckt sich auf die

öffentlichen Stellen des jeweiligen Landes sowie alle übrigen Unternehmen, die in dem jeweiligen Land ihren Sitz haben. Daneben bestehen auf der Grundlage der Art. 85 Abs. 2 und Art. 91 Abs. 2 DSGVO die Aufsichtsbehörden für die Bereiche Medien (insbesondere Rundfunk) und Kirche.

Nach dem BDSG fällt dem BfDI die Aufgabe zu, auf die Zusammenarbeit der öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind, hinzuwirken (§ 16 Abs. 5). Das in § 18 BDSG geregelte Verfahren soll gewährleisten, dass alle Behörden die Regel für das Kohärenzverfahren nach Art. 63 DSGVO einhalten und im Rahmen dessen wirksam beteiligt werden. Die deutschen Aufsichtsbehörden sprechen im Kohärenzverfahren sowie im Europäischen Datenausschuss (EDSA) mit einer Stimme. Vor der Übermittlung eines gemeinsamen Standpunktes an die Aufsichtsbehörden der anderen Mitgliedsstaaten, die EU-Kommission oder den EDSA geben sich die Aufsichtsbehörden des Bundes und der Länder frühzeitig Gelegenheit zur Stellungnahme (Satz 3). Die spezifischen Aufsichtsbehörden für die Bereiche Medien und Kirche werden beteiligt, sofern sie von der Angelegenheit betroffen sind (Satz 4).

Die Datenschutzaufsichtsbehörden im öffentlich-rechtlichen Rundfunk sehen die Vorschrift des § 18 Abs. 1 Satz 3 BDSG nur als bedingt geeignet an, die von Art. 63 DSGVO angestrebte Kohärenz zu gewährleisten, denn dem BDSG ist kein Anhaltspunkt dafür zu entnehmen, unter welchen Voraussetzungen sie von einer entsprechenden Angelegenheit „betroffen“ sein sollen. Aus der DSGVO ergibt sich eine dahingehende Anforderung nicht. Es ist deshalb fraglich, ob sie mit dem Sinn und Zweck der Art. 60 ff. DSGVO vereinbar ist.

Im Mai 2019 hatte die Datenschutzkonferenz der staatlichen Datenschutzbeauftragten (DSK) beschlossen, sich regelmäßig zweimal jährlich mit den spezifischen Aufsichtsbehörden auszutauschen. Corona-bedingt fand im Jahr 2020 nur ein Treffen, am 21.10.2020, mit den spezifischen Aufsichtsbehörden statt. Für die RDSK nahmen die Rundfunkdatenschutzbeauftragten von MDR, SWR und NDR sowie der Rundfunkdatenschutzbeauftragte von BR, SR, WDR, DRL und ZDF teil. Thematisiert wurden u. a. die Konsequenzen aus dem EuGH-Urteil ‚Schrems II‘; außerdem fand ein Austausch über Themen im Zusammenhang mit der Verarbeitung personenbezogener Daten bei der Bewältigung der Corona-Pandemie statt.

Wie schon im letzten Tätigkeitsbericht erwähnt, hat die DSK auch ihre Arbeitskreise für die spezifischen Aufsichtsbehörden geöffnet. Allerdings lassen die Arbeitskreise eine Beteiligung der Vertreter der RDSK nur auf Basis eines Gaststatus zu. Auf allen wesentlichen Sitzungen, die überwiegend virtuell stattfanden, war die RDSK zumindest durch eine Kollegin bzw. einen Kollegen vertreten.

L. Teilnahme an Fortbildungen und Veranstaltungen

Im Berichtszeitraum hat die Datenschutzbeauftragte zur Erhaltung und Erweiterung ihres Fachwissens an folgenden Fortbildungsveranstaltungen teilgenommen:

- Online-Veranstaltung des Bundesministeriums des Innern, für Bau und Heimat und der DSK zum Europäischen Datenschutztag 2021 "Transborder transfers – Herausforderungen des internationalen Datentransfers aus Sicht der Datenschutzkonvention 108+ und der DSGVO" am 28.1.2021

- Webinar der Stiftung Datenschutz zum Thema „Synthetische Daten: KI trainieren ohne Personenbezug" am 23.2.2021

- Online-Seminar des Instituts für Europäisches Medienrecht zum Online-Datenschutz (TTDSG-Entwurf) am 24.2.2021

- DatenDialog Online der Stiftung Datenschutz zur Datenstrategie der Bundesregierung am 16.3.2021

- Online-Veranstaltung der Stiftung Datenschutz zur Datenschutz-Folgenabschätzung – Praktische Umsetzung am Beispiel von Microsoft 365 am 25.3.2021

Berlin, im Mai 2021

gez. Anke Naujock-Simon

Anlagen:

1. Empfehlungen der RDSK – Folgerungen aus dem Urteil des EuGH zur Übermittlung personenbezogener Daten in Drittländer (‚Schrems II‘); Stand August 2020
2. Empfehlungen der RDSK zum Einsatz von Cookies in Online-Angeboten der Rundfunkanstalten; Stand September 2020
3. Datenschutzrechtliche Eckpunkte zum Einsatz von Kollaborationssystemen; Stand Februar 2021
4. Entschließung der RDSK zu Clubhouse; Stand Februar 2021

Anlage 1

Rundfunkdatenschutzkonferenz
RDSK
ARD | ZDF | Deutschlandradio

Empfehlungen der RDSK

Folgerungen aus dem Urteil des Europäischen Gerichtshofs zur Übermittlung personenbezogener Daten in Drittländer („Schrems II")

Mit Urteil vom 16.07.2020 (Az: C-311/18) hat der EuGH den Beschluss 2016/1250 der Kommission über die Angemessenheit des vom EU-US Datenschutzschild (Privacy Shield) gebotenen Schutzes für unwirksam erklärt. Damit kann das Privacy Shield Abkommen nicht mehr als Grundlage für Datenübermittlungen in die USA herangezogen werden. Die EU-Standardvertragsklauseln sind nach Auffassung des Gerichtshofs hingegen weiterhin gültig. Er hat jedoch betont, dass sowohl der verantwortliche Datenexporteur als auch der Datenimporteur prüfen muss, ob das gemäß den Standardvertragsklauseln unionsrechtlich geforderte Schutzniveau in dem Drittland, in das Daten übermittelt werden, überhaupt eingehalten werden kann oder ob zusätzliche Garantien geschaffen bzw. vereinbart werden müssen. Nähere Hinweise zu den gegebenenfalls erforderlichen weiteren Maßnahmen/Garantien enthält das Urteil nicht.

Diese Entscheidung stellt jeden Verantwortlichen in Europa vor die große Schwierigkeit, wie weiterhin Daten in die USA übermittelt werden können, ohne gegen geltendes Recht zu verstoßen. Die RDSK sieht die Politik und insbesondere die Europäische Kommission in der Pflicht, mit den USA ein neues Abkommen auszuhandeln, das den Anforderungen des europäischen Datenschutzrechts vollumfänglich entspricht.

Der Europäische Gerichtshof hat festgestellt, dass die Aufsichtsbehörden verpflichtet sind, eine Übermittlung personenbezogener Daten an ein Drittland auszusetzen oder zu verbieten, wenn sie der Auffassung sind, dass der nach dem Unionsrecht erforderliche Schutz nicht anders gewährleistet werden kann. Der Gerichtshof hat keine Übergangsfrist zugelassen.

Der RDSK ist bewusst, dass die Rundfunkanstalten nicht unmittelbar die Datenflüsse in Drittländer, insbesondere die USA stoppen können. Jedoch sind sie nach der Entscheidung des EuGH verpflichtet, die Datenübermittlungen an Drittstaaten, insbesondere die USA auf den Prüfstand zu stellen und wo immer notwendig weitere Maßnahmen, wie nachfolgend skizziert, zu ergreifen.

Die RDSK empfiehlt den Verantwortlichen insoweit folgendes Vorgehen:

1. Das EU-US Privacy Shield ist nicht mehr gültig, weshalb eine allein darauf fußende Datenübermittlung in die USA rechtswidrig ist. Die Rundfunkanstalten sind vor einer weiteren Datenübermittlung im Sinne der folgenden Ziffern aufgerufen, andere Rechtsgrundlagen für die Datenübermittlung zu finden, geeignete technische Maßnahmen zu ergreifen und/oder nach einer Alternative für die jeweilige Datenverarbeitung zu suchen.
2. Der EuGH hat die Gültigkeit der Standardvertragsklauseln nicht beschränkt. Er hat jedoch darauf hingewiesen, dass auf Seiten der Verantwortlichen eine Prüfpflicht ebenso besteht

wie bei dem Empfänger der Daten. Diese bezieht sich darauf, ob zusätzliche Garantien geschaffen bzw. vereinbart werden müssen, um das in den Standardvertragsklauseln geforderte Schutzniveau auch tatsächlich zu erreichen. Der Verantwortliche sollte im ersten Schritt eine Bestandsaufnahme der Datenübermittlung in Länder außerhalb des europäischen Wirtschaftsraumes und insbesondere in die USA durchführen. Eine Neubewertung der jeweiligen Datenverarbeitung ist angezeigt hinsichtlich ihrer Art, des Umfangs, des Zwecks der Verarbeitung sowie der vorgesehenen Empfänger. Maßgeblich für die Bewertung muss dabei der risikobasierte Ansatz sein, der die DSGVO prägt. In Hinblick auf die zu ergreifenden Maßnahmen kommt es also z. B. darauf an, ob nur wenige und vergleichsweise unkritische Daten in dem Drittland verarbeitet werden.

Bei Verwendung der Standardvertragsklauseln sollte der Verantwortliche den Empfänger der Daten (Datenimporteur) auffordern, offenzulegen ob und in ggf. welcher Weise er Auskunftspflichten gegenüber US-Behörden oder Geheimdiensten unterliegt. Im Ergebnis hat der Verantwortliche zu beurteilen, ob diese Eingriffe im Lichte der europäischen Gesetzgebung als verhältnismäßig anzusehen sind. Zu berücksichtigen hat er auch, ob der Datenimporteur zusichert, ihn über einen etwaigen Zugriff durch US-Behörden zu informieren und gegen unverhältnismäßige Zugriffe rechtlich vorzugehen.

3. Zu prüfen hat der Verantwortliche überdies, ob durch geeignete technische ggf. auch organisatorische Maßnahmen ein Zugriff der US-Behörden verhindert werden kann. Hier kommen insbesondere wirksame Verschlüsselungstechniken wie Ende-zu-Ende-Verschlüsselungen in Betracht.

4. Die Angemessenheitsbeschlüsse der EU-Kommission sind in den Blick zu nehmen. In diesen Beschlüssen wird festgestellt, dass personenbezogene Daten in einem bestimmten Drittland einen mit dem europäischen Datenschutzrecht vergleichbaren Schutz genießen. Unter folgendem Link sind die betroffenen Länder einzusehen: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_de
   Eine Verlagerung der Datenübermittlung und –verarbeitung in diese Länder ist unkritisch.

5. Die Feststellungen des Gerichtes beziehen sich allein auf den EU-US Privacy Shield sowie die Standardvertragsklauseln. Daher bleiben alle weiteren von der DSGVO vorgesehenen Garantien des Artikel 46 DSGVO weiterhin anwendbar.
   Insbesondere können eigenständige Vertragsklauseln vereinbart werden, die jedoch von der Genehmigung der jeweils zuständigen Datenschutzaufsicht abhängig sind.

6. Ausnahmsweise kann auch eine Datenübermittlung in Drittstaaten gemäß Artikel 49 DSGVO gerechtfertigt sein. Voraussetzung ist eine nur gelegentliche und nicht wiederholte Übermittlung. Dies ist schon dann nicht der Fall, wenn die Datenübermittlung im Rahmen einer dauerhaften Vertragsbeziehung stattfindet. Hierzu gibt es eine Auslegungshilfe des Europäischen Datenschutzausschusses (https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-22018-derogations-article-49-under-regulation_de).

Rundfunkdatenschutzkonferenz
RDSK
ARD | ZDF | Deutschlandradio

Die RDSK weist darauf hin, dass es sich bei dieser Empfehlung um eine erste Einschätzung handelt, die sie je nach Entwicklung der Rechtslage aktualisieren wird.

Stand: August 2020

Anlage 2

Rundfunkdatenschutzkonferenz
RDSK
ARD | ZDF | Deutschlandradio

EMPFEHLUNGEN ZUM EINSATZ VON COOKIES IN ONLINE-ANGEBOTEN DER RUNDFUNKANSTALTEN

September 2020

Der Europäische Gerichtshof (EuGH) hat am 1. Oktober 2019 – C 673/17 – die Anforderungen an eine wirksame Einwilligung zur Speicherung von oder den Zugriff auf Informationen konkretisiert, die bereits im Endgerät des Nutzers einer Website gespeichert sind. Nach Auffassung des Bundesgerichtshofs (BGH, Urt. vom 28. Mai 2020 – I ZR 7/16 -) gelten diese Grundsätze auch für Cookies, die Dienstanbieter einsetzen, um mithilfe von Pseudonymen Nutzungsprofile für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien zu erstellen. § 15 Abs. 3 Telemediengesetz (TMG) lässt Cookies zu diesen Zwecken zwar dem Wortlaut nach vorbehaltlich eines ausdrücklichen nutzerseitigen Widerspruchs zu; dies interpretiert der BGH jedoch im Sinne der Vorgaben von Art. 5 Abs. 3 ePrivacy-Richtlinie als Einwilligungserfordernis.

Aus dieser Rechtsprechung ergeben sich aus der Sicht der RDSK die folgenden Konsequenzen und Empfehlungen für den Einsatz von Cookies in den Angeboten der Rundfunkanstalten, insbesondere soweit es um die Nutzungsmessung zu publizistischen Zwecken geht.

I. GRUNDSÄTZLICHES ZUM EINSATZ VON COOKIES

1. Wann ist eine Einwilligung wirksam

Auf eine Einwilligung kann sich der Verantwortliche berufen, wenn die betroffene Person die entsprechende Erklärung zweifelsfrei aktiv, freiwillig und in Kenntnis aller für die Datenverarbeitung relevanten Umstände abgegeben hat. Diese Voraussetzungen sind im allgemeinen nur dann erfüllt, wenn der Verantwortliche die Person über die mit dem Cookie verbundene Datenverarbeitung umfassend informiert hat. Außerdem muss er ihr die Möglichkeit geben, das Einverständnis durch eigenes Handeln bzw. eine eigene Willenserklärung zu erteilen, etwa durch Ankreuzen eines entsprechenden Kästchens. Wenn sich die Person gegen die Einwilligung entscheidet, darf sich das für sie nicht nachteilig auswirken.

Die Person muss die Einwilligungserklärung leicht als solche erkennen können. Das schließt zwar nicht aus, dass der Verantwortliche sie mit weiteren Willensbekundungen verbindet. Dann muss die Einwilligungserklärung aber von den anderen Sachverhalten klar unterscheidbar sein.

Eine Einwilligung kann sich auch auf mehrere Cookies beziehen, wenn diese jeweils denselben Zweck verfolgen.

2. In welchen Fällen ist eine Einwilligung einzuholen

a) Art. 6 Abs. 1 S. 1 DSGVO

Nach der Systematik des Art. 6 Abs. 1 DSGVO benötigt der Verantwortliche für die Verarbeitung personenbezogener Daten immer dann die Einwilligung des Betroffenen, wenn er sich nicht auf

einen der gesetzlichen Erlaubnistatbestände stützen kann, die Art. 6 Abs. 1 S. 1 lit. b) bis f) DSGVO nennt.

b) Art. 5 Abs. 3 S. 1 ePrivacy-Richtlinie, § 15 Abs. 3 TMG

Während die DSGVO die Grundrechte und -freiheiten natürlicher Personen schützt, dient Art. 5 Abs. 3 ePrivacy-RiLi und damit § 15 Abs. 3 TMG dem Schutz der Privatsphäre der Nutzer unabhängig davon, ob es dabei um personenbezogene Daten geht. Nach der Rechtsprechung des BGH würden die Rundfunkanstalten nach dieser Vorschrift eine Einwilligung benötigen, wenn sie Cookies einsetzen, mithilfe derer sie „pseudonymisierte Nutzungsdaten der betroffenen Person für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung ihres Online-Angebots" auswerten.

3. Wann ist keine Einwilligung erforderlich

a) Unbedingt erforderliche Cookies

Eine Einwilligung ist nicht nötig, wenn die mit dem Einsatz des Cookies verbundene Speicherung oder der Zugang zu den entsprechenden Daten unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann.

Danach bedürfen jedenfalls sogenannte ‚funktionale Cookies' keiner Einwilligung, die etwa

- dem Verantwortlichen eine (technische) Fehleranalyse ermöglichen,
- der Sicherheit seines Angebots dienen,
- die Login-Daten seiner Nutzer speichern,
- für Transaktionen (Warenkorbfunktion) oder
- zur Individualisierung von Webseiteninhalten erforderlich sind.

b) Sonstige Cookies

Der Verantwortliche benötigt keine Einwilligung, wenn er personenbezogene Daten unter den in Art. 6 Abs. 1 S. 1 lit. b) bis f) DSGVO genannten Voraussetzungen verarbeitet. Diese Erlaubnistatbestände betreffen aber jeweils sehr spezifische Sachverhalte und kommen deshalb für den Einsatz von Cookies nur in besonders gelagerten Fällen in Betracht.

II. EINSATZ VON COOKIES ZUR ANONYMISIERTEN NUTZUNGSMESSUNG

1. Zulässigkeit nach Art. 6 Abs. 1 S. 1 lit. e) und f) DSGVO

Der öffentlich-rechtliche Rundfunk verbreitet Telemedien, um seinen verfassungsrechtlichen Funktionsauftrag zu erfüllen. Nach der Rechtsprechung des Bundesverfassungsgerichts darf (und muss) er sein von den Beitragszahlern finanziertes Angebot im gesellschaftlichen Interesse auf allen publizistisch relevanten Plattformen zugänglich machen. Ob, wo und wie er damit seinen publizistischen Auftrag erfüllt, hängt von der Konfiguration dieses Angebots ab. Die Rundfunkanstalten sind dazu auf Erkenntnisse zur Akzeptanz und Nutzung ihres Angebots angewiesen. Dies gilt allerdings ausschließlich für anonymisierte Auswertungen, wie sie auch im linearen Rundfunk

üblich sind. Vergleichbar statistisch belastbare Methoden wie etwa die Messung der Zuschauerquote (Fernsehen) oder die Media-Analyse (Hörfunk) stehen dafür im Online-Bereich jedoch bislang nicht zur Verfügung. Die Rundfunkanstalten haben daher im Rahmen ihres verfassungsrechtlichen Funktionsauftrags ein berechtigtes Interesse am Einsatz von Cookies, die diese Aufgabe für ihr Onlineangebot übernehmen. Sie verfolgen damit kein (markt-)wirtschaftliches, sondern ein ausschließlich publizistisches Ziel.

Für die Rundfunkanstalten ist die anonymisierte Nutzungsmessung daher erforderlich, damit sie die ihnen durch Art. 5 Abs. 1 S. 2 GG übertragene Aufgabe optimal wahrnehmen können, Art. 6 Abs. 1 S. 1 lit. e) DSGVO. Auch nach Maßgabe einer Interessenabwägung gemäß Art. 6 Abs. 1 S. 1 lit. f) DSGVO ist die Nutzungsmessung zulässig. Nach dem Urteil des EuGH vom 1.10.2019 kann das allgemeine Interesse des Verantwortlichen an einer Erfassung und Auswertung des Nutzungsverhaltens (insbesondere für die in § 15 Abs. 3 TMG genannten Zwecke) zwar nicht per se als „berechtigtes Interesse" im Sinne von Art. 6 Abs. 1 S. 1 lit. f) DSGVO qualifiziert werden. Im Falle einer ausschließlich publizistisch motivierten anonymisierten Nutzungsmessung überwiegt jedoch das Interesse der Rundfunkanstalt (und der Gesamtheit ihres Publikums) ein etwa entgegenstehendes individuelles Interesse, Art. 6 Abs. 1 S. 1 lit. f) DSGVO.

2. Kein Einwilligungserfordernis nach § 15 Abs. 3 TMG

§ 15 Abs. 3 TMG sollte es Telemedienanbietern ursprünglich ermöglichen, auch ohne Einwilligung pseudonymisierte Nutzungsprofile „für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung ihrer Telemedien" anzulegen. Nach ihrem Sinn und Zweck zielte die Vorschrift darauf, dem Verantwortlichen das Anlegen personalisierbarer Nutzerprofile für die genannten Zwecke zu erleichtern. Eine anonymisierte Nutzungsmessung ermöglicht den Rundfunkanstalten jedoch keine personalisierbare, sondern ausschließlich eine auf ihr Onlineangebot insgesamt bezogene statistische Auswertung. Daher unterfällt die Nutzungsmessung der Rundfunkanstalten nicht dem Anwendungsbereich des § 15 Abs. 3 TMG und dem nach Auffassung des BGH dort postulierten Einwilligungserfordernis.

III. EMPFEHLUNGEN FÜR DIE RUNDFUNKANSTALTEN

Rechtsgrundlage prüfen
Die Rundfunkanstalten sollten jedes von ihnen eingesetzte Cookie darauf überprüfen, ob sie es auf einen Erlaubnistatbestand stützen können. Dies kann einer der in Art. 6 Abs. 1 S. 1 lit. b) - f) DSGVO genannten Tatbestände und muss ansonsten stets eine Einwilligung der betroffenen Person sein.

Wirksamkeit der Einwilligungserklärung sichern
Die Rundfunkanstalten sollten die von ihnen eingesetzten Tools, mithilfe derer sie die im Regelfall erforderliche Einwilligung der betroffenen Person einholen, daraufhin überprüfen, ob sie die Anforderungen erfüllen, die sich aus Art. 4 Nr. 11, Art. 7 und ggf. Art. 8 DSGVO sowie der Rechtsprechung des EuGH ergeben.

Rundfunkdatenschutzkonferenz
RDSK
ARD | ZDF | Deutschlandradio

Datenschutzerklärung/Cookie-Hinweis anpassen
Die Datenschutzerklärung muss Hinweise zur Funktion des jeweiligen Cookies mit mindestens allen Angaben enthalten, die Art. 13 DSGVO fordert.

Spezifische Aufgabe des öffentlich-rechtlichen Rundfunks erklären
Zurecht erwarten die Nutzer vom öffentlich-rechtlichen Rundfunk einen besonders hohen Datenschutzstandard. Da im allgemeinen gerade Cookies, die das Nutzungsverhalten erfassen und auswerten, nur mit ausdrücklicher Einwilligung der betroffenen Person eingesetzt werden dürfen, entsteht erhöhter Aufklärungs- und Beratungsbedarf, wenn die Rundfunkanstalten weiterhin für einzelne Cookies keine Einwilligung einholen. Sie sollten daher ihre Datenschutzerklärungen bzw. Cookie-Hinweise besonders sorgfältig und verständlich formulieren. Allgemeinplätze wie etwa das Bestreben, mithilfe eines Cookies „den Nutzern ein bestmögliches Angebot zur Verfügung zu stellen", werden dem nicht gerecht. Insbesondere sollten die Rundfunkanstalten daher die spezifische Aufgabe und Funktion des öffentlich-rechtlichen Rundfunks erläutern und die sich daraus ergebende Rechtsgrundlage für den Einsatz des betreffenden Cookies nennen.

Anlage 3

Rundfunkdatenschutzkonferenz
RDSK
ARD | ZDF | Deutschlandradio

Datenschutzrechtliche Eckpunkte zum Einsatz von Kollaborationssystemen

Stand: Februar 2021

I. Ausgangslage

Spätestens seit dem Inkrafttreten der coronabedingten Abstandsregelungen ist der Einsatz elektronischer Plattformen, die die ortsunabhängige Kommunikation und Zusammenarbeit zwischen mehreren Beteiligten ermöglichen (im Folgenden: Kollaborationssysteme) in den Fokus gerückt. Sie ermöglichen u. a. die folgenden Funktionen: Mailversand, Telefon- und Videokonferenz, Teamräume, Chats sowie gemeinsame Bearbeitung von Dokumenten. Besonders hoch ist die Nachfrage nach Videokonferenzen für Besprechungen, virtuelle Versammlungen, Bewerbungsgespräche, Publikumsbefragungen und vieles mehr. Angesichts der erheblichen Vorteile der virtuellen Kommunikation und Zusammenarbeit ist damit zu rechnen, dass die Kollaborationssysteme dauerhaft wichtige Werkzeuge für die Zusammenarbeit im öffentlich-rechtlichen Rundfunk und mit Externen bleiben werden.

Der Einsatz derartiger Plattformen muss allerdings datenschutzkonform sein. Denn bei ihrer Nutzung werden insbesondere folgende personenbezogene Daten verarbeitet:

- Namen und Kontaktdaten der User*innen
- Inhalte der Videokonferenz, also Ton und (Bewegt-)Bild, des Chats, der Dateien (Dokumente); dazu können auch besonders sensible Daten im Sinne von Art. 9 DSGVO gehören (z. B. körperliche Eigenschaften, politische Einstellungen etc.).
- Metadaten (z.B. zum konkreten Standort oder verwendeten Rechner)

II. Anforderungen in datenschutzrechtlicher Hinsicht

1. Schutzbedarfsfeststellung

Vor einer Auswahlentscheidung für ein Kollaborationssystem muss der Verantwortliche (im Folgen- den: die Rundfunkanstalt) das angemessene Schutzniveau für die personenbezogenen Daten festlegen, die mittels der Plattform – voraussichtlich – verarbeitet werden. Die an das System zu stellen- den Anforderungen in datenschutzrechtlicher Hinsicht richten sich nach dem Schutzbedarf der Daten, den die Rundfunkanstalt auf dieser Grundlage festgestellt hat. Ausschlaggebend ist die am höchsten ermittelte Schutzklasse der einzelnen Datenkategorien. Gegebenenfalls muss die Rundfunkanstalt durch geeignete technische und/oder organisatorische Maßnahmen verhindern, dass eine Kollaborationsplattform für Zwecke bzw. Anlässe genutzt wird, bei denen nicht hinreichend gewährleistet ist, dass personenbezogene Daten verarbeitet werden, die einer höheren Schutzklasse als der zugelassenen unterliegen (siehe auch III.).

2. Datenschutzrechtliche Anforderungen

Die Kollaborationsplattform muss alle zwingenden datenschutzrechtlichen Anforderungen, insbesondere die Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 DSGVO, u. a. Transparenz, Zweckbindung und Datensparsamkeit) sowie für die Rechtmäßigkeit der Verarbeitung (Art. 6 DSGVO) erfüllen. Die Möglichkeit datenschutzfreundlicher Voreinstellungen (Art. 25 DSGVO) muss gegeben sein. Unter den in Art. 35 DSGVO genannten Voraussetzungen muss die Rundfunkanstalt dazu gegebenenfalls eine Datenschutzfolgenabschätzung durchführen. Eine solche ist jedenfalls erforderlich, wenn das betreffende System den Einsatz neuer Technologien wie Sprach-, Gesichts- oder Stimmerkennung oder die Transkription ermöglicht bzw. vorsieht.

3. Betriebsmodelle

Grundsätzlich kann die Rundfunkanstalt wählen, ob sie eine Kollaborationsplattform selbst oder gemeinsam mit anderen Rundfunkanstalten oder Einrichtungen betreibt, oder aber den Online-Dienst eines externen Anbieters nutzt. Sofern sie sich für einen externen Dienstleister entscheidet, muss sie allerdings Folgendes beachten:

Je nachdem, um welches Fremdsystem es sich handelt, werden bei dessen Nutzung personenbezogene Daten ganz oder teilweise auf Server in Nicht-EU-Staaten, insbesondere in die USA übermittelt. Der EuGH hat mit Urteil vom 16. Juli 2020 („Schrems II") die Privacy Shield-Vereinbarung für unwirksam erklärt und hält zudem auch die von der EU-Kommission bislang entwickelten Standardvertragsklauseln ohne zusätzliche Garantien und Maßnahmen für keine hinreichende Rechtsgrundlage für den Datentransfer in die USA. Empfehlungen zu dahingehenden technischen und vertraglichen Maß- nahmen hat der Europäische Datenschutzausschuss (EDSA) am 10. November 2020 veröffentlicht (https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplemen tarymeasurestransferstools_en.pdf).

Daraus folgt, dass Systeme von US-Anbietern wie Microsoft, Zoom oder anderen nur dann DSGVO- konform genutzt werden können, wenn die Rundfunkanstalt neben der Vereinbarung der Standardvertragsklauseln zusätzliche Garantien und Maßnahmen durchsetzt, die ein der DSGVO entsprechen- des Datenschutzniveau gewährleisten.

Eine Einschränkung gilt für die Verarbeitung von streng vertraulichen personenbezogenen Daten:

Soll eine Kollaborationsplattform (auch) eingesetzt werden können, um streng vertrauliche personenbezogene Daten der Rundfunkanstalt (z. B. sensible Gesundheitsdaten oder Recherchematerial aus dem investigativen Bereich) zu verarbeiten, so ist die Wahlmöglichkeit bezüglich der Betriebsmodelle eingeschränkt. Streng vertrauliche personenbezogene Daten müssen vollständig vor dem Zugriff Externer –

einschließlich dem des externen Dienstleisters – geschützt sein, z. B. durch Ende- zu-Ende-Verschlüsselung. Dies gilt insbesondere für externe Dienstleister, die ihren Sitz außerhalb der EU haben und die Anforderungen der DSGVO nicht vollständig erfüllen können. Kann ein Zugriff des externen Dienstleisters nicht vollständig ausgeschlossen werden, so muss die Rundfunkanstalt ggf. im Verbund mit den anderen Rundfunkanstalten für diese streng vertraulichen personenbezogenen Daten ein eigenes System betreiben.

4. Auftragsverarbeitung

Entscheidet sich die Rundfunkanstalt für eine durch einen externen Dienstleister betriebene Kollaborationsplattform, so wird der Anbieter in datenschutzrechtlicher Hinsicht als Auftragsverarbeiter für sie tätig. Grundlage dafür ist ein Auftragsverarbeitungsvertrag, der die Anforderungen des

Art. 28 DSGVO, insbesondere Abs. 3 lit. a) - g) DSGVO erfüllen muss. Abhängig vom Ergebnis der Schutzbedarfsfeststellung muss die Rundfunkanstalt angemessene technische und organisatorische Maßnahmen (TOM) zur Gewährleistung der Informationssicherheit vereinbaren bzw. ergreifen. Dazu gehören namentlich folgende Anforderungen an die Nutzung der Kollaborationsplattform:

- Ausschalten des Aktivitätstrackings von Teilnehmer*innen
- Möglichkeit für manuelle Datenschutzeinstellungen der Nutzer*innen entsprechend der internen Vorgaben der Rundfunkanstalt
- Transportverschlüsselung nach dem Stand der Technik
- Möglichkeit der Deaktivierung von Mitschnitten einer Videokonferenz und die Möglichkeit der Vorabinformation an die Teilnehmer*innen über die Aufzeichnung
- Automatische bzw. entsprechend den Aufbewahrungsbestimmungen festgelegte Löschung eventueller Aufzeichnungen bzw. Mitschnitte nach einer Videokonferenz
- Deaktivierung der Möglichkeit zur Erstellung von Nutzungsprofilen
- Möglichkeit einer Hintergrundweichzeichnung oder eines virtuellen Hintergrundes
- Nutzerbezogener Zugang mit sicherem Authentisierungsverfahren nach dem Stand der Technik; bei Zugriff außerhalb der Rundfunkanstalt Multi-Faktor-Authentifizierung

Sofern der Anbieter seinen Sitz in einem Nicht-EU-Staat hat bzw. die Daten in einem Nicht-EU-Staat verarbeitet, muss die Rundfunkanstalt überdies prüfen, ob die Datenübermittlung in das Drittland im Einklang mit den Art. 44 ff. DSGVO steht (Näheres dazu siehe Ziffer 3).

Außerdem muss die Rundfunkanstalt ausschließen, dass der Auftragsverarbeiter die beim Betrieb seiner Plattform verarbeiteten personenbezogenen Daten ohne ordnungsgemäße Einwilligung der jeweils Beteiligten bzw. ohne gesetzliche Grundlage für eigene Zweck nutzt.

III. Organisatorische Maßnahmen zur Einhaltung von Datenschutz und Informations- sicherheit

In einem internen Regelwerk (Dienstanweisung, Betriebs- oder Dienstvereinbarung) sollte die Rundfunkanstalt die einzuhaltenden technischen und organisatorischen Maßnahmen (TOM) zur Gewährleistung von Datenschutz und Datensicherheit für die Administrator*innen und alle Anwender*innen verpflichtend festhalten. Zu den dort zu regelnden Punkten sollten insbesondere gehören:

- Überblick über die datenschutzrechtlichen Risiken bei der Nutzung von Kollaborationsplattformen (Information und Sensibilisierung)
- Freigabeverfahren, das festlegt, welche Kollaborationsplattformen für die Verarbeitung welcher Datenklassen freigegeben sind bzw. welche Voraussetzungen an die Freigabe gestellt sind
- datenschutzfreundliche Voreinstellungen (z. B. Kamera und Mikrofon deaktiviert) als vorgegebener Standard
- Vorgaben zum Funktionsumfang und zu Zugriffsberechtigungen, darunter etwa die Verpflichtung zur Prüfung, ob anstatt einer Video- eine Telefonkonferenz ausreicht, Einschränkungen bzw. Modalitäten zur Nutzung der Aufzeichnungsfunktion (Mittschnitt, Screenshot, Fotografie)
- Möglichkeit, den Zugang zu Konferenzen zu schützen (z. B. Registrierung, Passwort)
- Möglichkeit der Vorfilterung externer Teilnehmer*innen (z. B. virtueller Wartebereich für Gäste bzw. Externe)
- Geeignete und verlässliche Information aller Konferenzteilnehmer*innen über die Identität der Teilnehmer*innen
- Gewährleistung, dass alle personenbezogenen Daten nach Ablauf festgelegter Löschfristen effektiv gelöscht werden
- Ausschluss einer Auswertung der Daten zur Verhaltens- oder Leistungskontrolle.

IV. Dokumentation und Information

Die für den Einsatz der jeweiligen Kollaborationsplattform verantwortliche Rundfunkanstalt muss die Anwendung gemäß Art. 30 DSGVO in ihrem Verarbeitungsverzeichnis dokumentieren (Art. 5 Abs. 2 DSGVO) und außerdem ihre zur Nutzung des Systems berechtigten oder verpflichteten Beschäftigten über die mit dem Einsatz eines solchen Systems verbundenen datenschutzrelevanten Aspekte um- fassend und verständlich informieren. In den Fällen, in denen die Datenverarbeitung via Kollaborationsplattform auf die Einwilligung der Beteiligten (etwa aus anderen Rundfunkanstalten oder sonstigen Organisationen) gestützt werden soll (Art. 6 Abs. 1 lit. a) DSGVO), muss die Rundfunkanstalt die Voraussetzungen zur Einholung einer rechtswirksamen Einwilligung schaffen. Im Falle einer Verletzung des Schutzes personenbezogener Daten beim Einsatz eines solchen Systems unterliegt die jeweils verantwortliche Rundfunkanstalt der Meldepflicht nach Art. 33 DSGVO.

Anlage 4

Rundfunkdatenschutzkonferenz
RDSK
ARD | ZDF | Deutschlandradio

Entschließung der RDSK zu „Clubhouse“

Clubhouse ist eine neue App für Audio-Talkshows. Über sie kann sich der App-Nutzer **Gespräche anhören und an Diskussionen teilnehmen**. Es sind öffentliche Diskussionen (vergleichbar virtuell gestalteten Podiumsdiskussionen), aber auch geschlossene Gruppen möglich. Ein Moderator spricht live über ein bestimmtes Thema und der Nutzer kann als Zuhörer teilnehmen. Er ist zunächst stumm geschaltet, kann aber vom Moderator zum Gespräch freigeschaltet werden. **Clubhouse ist** also eine **Art „Live-Talkshow“ ohne Kamera** (und Textnachrichten).

Datenschutzrechtlich ist diese neue App aus mehreren **Gründen** sehr **bedenklich**:

- **Zugriff auf Kontakte**
  Die App erfordert den Zugriff auf alle auf dem Gerät des Nutzers gespeicherten Kontakte, wenn dieser selbst zu einer Gesprächsrunde einladen will . Er muss also die **Kontaktdaten Dritter** (die neben den Telefonnummern auch E-Mail-Adressen und Wohnadressen sein können) auf dem Smartphone mit Clubhouse teilen. Damit erhält Clubhouse zum einen Informationen über das **soziale Umfeld** des Nutzers. Zum anderen werden die Kontaktdaten von Personen, die noch nicht bei Clubhouse registriert sind, ohne deren Einwilligung an das Unternehmen übermittelt. Bei der Anmeldung über einen Social-Media-Account behält sich Clubhouse den Zugang für Follower und Freundeslisten vor.

- **Audiomitschnitte und Speicherung in den USA**
  Clubhouse fertigt Audiomitschnitte, die nach eigenen Angaben ausschließlich zur Unterstützung der Untersuchung von Vorfällen aufgezeichnet werden. Diese werden ebenso wie die erhobenen Kontakt- und Accountinformationen der Nutzer und Dritter zumindest für gewisse Zeit **in den USA gespeichert** und verarbeitet sowie an verschiedene Unternehmen weitergegeben. Zusagen über ein der DSGVO vergleichbares angemessenes Niveau zum Schutz dieser Daten enthält die Datenschutzerklärung des Anbieters bislang nicht. Ohne entsprechende Vorkehrungen verstößt die Datenübermittlung in die USA gegen die DSGVO (vgl. das EuGH-Urteil vom 16.7.2020, C-311/18 zum Privacy Shield).

- **Fehlende Transparenz**
  In den Allgemeinen Geschäftsbedingungen („Terms of Service“) und der unzulässigerweise nur in englischer Sprache formulierten Datenschutzerklärung („Privacy Policy“) von Clubhouse wird die DSGVO bislang nicht erwähnt und eine Adresse für Datenschutzauskünfte in der EU bzw. ein Vertreter nach Art. 17 DSGVO nicht benannt. Ein **Tracking** kann wohl nicht verhindert werden und eine **Profilbildung des Nutzers** ist möglich. Wer zu den Empfängern der personenbezogenen Daten gehört und ob und in

welchem Umfang Daten an Geschäftspartner verkauft werden, ist unklar und wird nicht transparent kommuniziert.

Zusammenfassend lässt sich feststellen: Von der **Nutzung dieser App ist bis auf weiteres dringend abzuraten**. Die RDSK fordert die Rundfunkanstalten und ihre Beteiligungsunternehmen auf, die Installation der App auf allen dienstlich zur Verfügung gestellten Geräten, mindestens aber einen Zugriff der App auf das dienstliche Kontaktverzeichnis wirksam und vollständig zu unterbinden, bis der Anbieter eine DSGVO-konforme Nutzung ermöglicht hat.

Februar 2021