

TÄTIGKEITSBERICHT

der Datenschutzbeauftragten von Radio Bremen

Ivka Jurčević

für den Zeitraum vom

1. Januar 2021 bis zum 31. Dezember 2021

dem Rundfunkrat von Radio Bremen gemäß
§ 14 Satz 7 des Bremischen Ausführungsgesetzes
zur EU-Datenschutz-Grundverordnung
in seiner Sitzung am 31. März 2022 vorgelegt

Inhaltsverzeichnis

A. Einleitung	- 3 -
B. Die Datenschutzbeauftragte von Radio Bremen	- 4 -
C. Entwicklungen im Datenschutzrecht	- 6 -
I. Neue Standardvertragsklauseln	- 6 -
1. Allgemeines	- 6 -
2. Auswirkungen in der Praxis	- 8 -
II. Telekommunikation-Telemedien-Datenschutz-Gesetz	- 8 -
III. Stand: Entwurf einer e-Privacy-Verordnung	- 10 -
-	
D. Datenschutz bei Radio Bremen	- 10 -
I. Datenschutz in der Corona-Pandemie	- 10 -
1. Abfrage des Impf- und Genesenenstatus	- 11 -
2. 3G-Regelung am Arbeitsplatz	- 12 -
3. Weitere Beratung im Zusammenhang mit Corona-Maßnahmen	- 14 -
II. Datenschutz im Programmbereich	- 14 -
1. Kontaktdatenbank für die redaktionelle Einbindung von Expert*innen	- 14 -
2. Beanstandungen durch die Datenschutzbeauftragte	- 15 -
III. Datenschutz im Verwaltungsbereich	- 15 -
1. Einführung von Microsoft 365	- 15 -
a. Allgemeines	- 15 -
b. Arbeitsgruppe	- 16 -
c. Datenschutz und IT-Sicherheit	- 17 -
d. Änderungen der IT-Regelungen zur Ermöglichung der Nutzung von Cloud-Diensten	- 19 -
e. Weitere Schritte	- 19 -
2. Datenschutzrechtliche Schulungen der Mitarbeitenden	- 20 -
3. ARD-Mindeststandard zur Authentisierung von ARD und Deutschlandradio	- 21 -
4. SAP-Prozessharmonisierung „(D)ein SAP“	- 21 -

5. Arbeitsgruppe IT-Sicherheit	- 22 -
6. Datenschutzvorfälle	- 22 -
E. Auskunftsanfragen und Beschwerden	- 22 -
I. Auskunftsanfragen gemäß Art. 15 DSGVO	- 23 -
II. Beschwerden	- 23 -
F. Zusammenarbeit	- 24 -
I. Rundfunkdatenschutzkonferenz	- 24 -
II. Arbeitskreis der Datenschutzbeauftragten	- 26 -
III. Die Datenschutzkonferenz	- 27 -
IV. IVZ-Jahrestreffen	- 27 -
G. Fortbildungen	- 29 -

A. Einleitung

Der vorliegende Tätigkeitsbericht beschreibt und dokumentiert meine Tätigkeit als Datenschutzbeauftragte von Radio Bremen in der Zeit vom 1. Januar bis zum 31. Dezember 2021.

Gemäß § 14 Bremisches Ausführungsgesetz zu der EU-Datenschutz-Grundverordnung (BremDSGVOAG) hat die Beauftragte für den Datenschutz von Radio Bremen dem Rundfunkrat jährlich einen Bericht ihrer Tätigkeit zu erstatten.

Das vergangene Berichtsjahr stand erneut im Zeichen der Corona-Pandemie. Im Zusammenhang mit den vielfältigen Herausforderungen für Staat und Gesellschaft war dabei auch das Datenschutzrecht von Belang. Meine Tätigkeit umfasste daher zu einem großen Teil die datenschutzrechtliche Beratung bei der Umsetzung der Corona-Maßnahmen. Einen Prüfungsschwerpunkt bildete dabei die Zulässigkeit der Verarbeitung von Gesundheitsdaten, wie zum Beispiel die Abfrage des Impf- oder Genesenstatus in verschiedenen Arbeitszusammenhängen.

Neben der Befassung mit pandemiebedingten Themen war ich als Datenschutzbeauftragte in zahlreiche redaktionelle und betriebliche Angelegenheiten eingebunden. Die Schwerpunkte meiner Arbeit bildeten u.a. die Begleitung und Bewertung neuer informationstechnischer Systeme (IT-Systeme), allen voran Microsoft 365, sowie die Befassung mit datenschutzrechtlichen Einzelfragen aus den jeweiligen Fachbereichen.

Ferner war ich mit der Prüfung und Beantwortung von datenschutzrechtlichen Auskunftsanfragen sowie der Mitwirkung an hausinternen Arbeitsgruppen und ARD-weiten Arbeitskreisen bzw. Konferenzen beschäftigt.

Nachdem dieser Tätigkeitsbericht dem Rundfunkrat zur Kenntnisnahme vorgelegt worden ist, wird er im Online-Angebot von Radio Bremen unter folgendem Link veröffentlicht werden:

<https://dein.radiobremen.de/info/datenschutz/datenschutz-beauftragte-106.html>

Für die Unterstützung bei der Ausübung meines Amtes danke ich meinen Kolleg*innen aus dem Justizariat, dem Datenschutzbeauftragten der Bre-media Produktion GmbH und dem IT-Sicherheitsbeauftragten von Radio Bremen, mit denen ich seit Übernahme meines Amtes vertrauensvoll zusammenarbeite. Danken möchte ich ebenfalls dem Personalrat, der mit dafür Sorge trägt, dass die datenschutzrechtlichen Anforderungen berücksichtigt werden sowie allen Kolleg*innen, die die datenschutzrechtlichen Belange bei den jeweiligen Vorhaben frühzeitig im Blick haben und dadurch helfen, dass diese umgesetzt werden können.

B. Die Datenschutzbeauftragte von Radio Bremen

Ich bin am 25. Juni 2020 vom Rundfunkrat zur Datenschutzbeauftragten von Radio Bremen bestellt worden und übe dieses Amt neben meiner Tätigkeit als Juristin im Justizariat von Radio Bremen aus.

Gemäß § 14 S. 3 BremDSGVOAG habe ich darauf zu achten, dass die datenschutzrechtlichen Vorschriften, denen Radio Bremen bei der Verarbeitung von personenbezogenen Daten zu journalistischen Zwecken unterliegt, eingehalten werden. Im journalistisch-redaktionellen Bereich bin ich daher als Aufsichtsbehörde tätig. An mich kann sich jede Person wenden, die annimmt, bei der Verarbeitung personenbezogener Daten zu journalistischen Zwecken in ihren Rechten verletzt worden zu sein. Dies können Hörer*innen und Zuschauer*innen sowie Personen, die Gegenstand der Berichterstattung von Radio Bremen sind, sein.

Neben diesen Aufgaben als Aufsichtsbehörde im journalistisch-redaktionellen Bereich bin ich auch als betriebliche Datenschutzbeauftragte von Radio Bremen tätig und für die Sicherstellung des Datenschutzes im administrativ-verwaltenden Bereich zuständig. Diese Doppelfunktion ermöglicht § 14 S.5 BremDSGVOAG.

Die Aufsicht für die Verarbeitung personenbezogener Daten, die nicht zu journalistischen Zwecken erfolgt, obliegt dagegen der Landesbeauftragten für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen.

Ich bin in der Ausübung meines Amtes unabhängig und nur dem Gesetz unterworfen; im Übrigen unterstehe ich der Dienstaufsicht des Verwaltungsrates.

Die Aufgaben als Aufsichtsbehörde werden in den Art. 51 ff. EU-Datenschutzgrundverordnung (DSGVO) sowie in Art. 39 DSGVO für die betriebliche Datenschutzbeauftragte konkretisiert. Diese Vorschriften bilden neben § 14 BremDSGVOAG die weiteren Rechtsgrundlagen für meine Tätigkeit als Datenschutzbeauftragte von Radio Bremen.

C. Entwicklungen im Datenschutzrecht

Neue Entwicklungen im Datenschutzrecht gab es auf europäischer als auch auf nationaler Ebene.

I. Neue Standardvertragsklauseln

1. Allgemeines

Am 4. Juni 2021 hat die Europäische Kommission neue Standardvertragsklauseln, die sog. SCCs („Standard Contractual Clauses“), für den Datentransfer in Drittländer verabschiedet. (*Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates*). Als Drittländer gelten alle Staaten, die außerhalb der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) liegen, z.B. die USA.

Gemäß der DSGVO dürfen personenbezogene Daten nur dann in ein Drittland übermittelt werden, wenn dort ein angemessenes Datenschutzniveau für diese Daten besteht. Ein angemessenes Schutzniveau kann u.a. durch geeignete Garantien hergestellt werden. Eine von diesen Garantien sind die Standardvertragsklauseln gemäß Art. 46 Abs. 2 lit. c) DSGVO. Bei diesen handelt es sich um Musterverträge, in denen sich die Vertragsparteien verpflichten, ein der DSGVO vergleichbares Datenschutzniveau einzuhalten.

Hintergrund der Überarbeitung der bisherigen Standardvertragsklauseln war das „Privacy Shield“-Urteil des Europäischen Gerichtshofs (EuGH) vom 16. Juli 2020, über welches ich in meinem Tätigkeitsbericht 2020 unter Buchstabe C. Ziffer I. 1 berichtet habe. Darin erklärte der EuGH das „EU-US Privacy Shield“ (Datenschutzschild) für ungültig.

Das „EU-US Privacy Shield“ war bis dato die Grundlage für den Datentransfer aus der EU in die USA, um ein angemessenes Datenschutzniveau im Drittland nachzuweisen.

Die bisherigen Standardvertragsklauseln, die ebenfalls Gegenstand der Entscheidung waren, befand der EuGH zwar weiterhin für wirksam. Das Gericht stellte jedoch auch fest, dass die Standardvertragsklauseln wenig an den gesetzlichen Zugriffsmöglichkeiten durch US-Sicherheitsbehörden ändern. In den USA ermöglichen die verschiedenen US-Sicherheitsgesetze wie der „Patriot Act“ und der „Cloud Act“ unter anderem den Zugriff der amerikanischen Sicherheitsbehörden auf den Datenbestand von US-Unternehmen. Vor diesem Hintergrund hat der EuGH deutlich gemacht, dass auch unter Verwendung der Standardvertragsklauseln zusätzliche Maßnahmen notwendig sein können, um ein angemessenes Datenschutzniveau im Drittland zu gewährleisten. Nähere Hinweise zu den gegebenenfalls erforderlichen weiteren Maßnahmen enthielt das Urteil hingegen nicht.

Die überarbeiteten Standardvertragsklauseln berücksichtigen das vorgenannte EUGH-Urteil und bringen einige Erweiterungen und Änderungen mit sich. Die Problematik, dass Behörden in einem Drittland gegebenenfalls auf personenbezogene Daten zugreifen, wird aber auch durch die neuen Standardvertragsklauseln nicht vollständig gelöst. Aufgrund ihrer Rechtsnatur als Vertrag binden die Standardvertragsklauseln nämlich nur die Vertragsparteien und nicht die Behörden. Soweit der Schutz der personenbezogenen Daten und die Rechte der Betroffenen auf Grundlage der Standardvertragsklauseln nicht ausreichend gewahrt werden können, sind weiterhin zusätzliche Maßnahmen erforderlich. Die überarbeiteten Standardvertragsklauseln enthalten nun Beispiele für mögliche zusätzliche Schutzmaßnahmen, u.a. technische Maßnahmen wie die Verschlüsselung personenbezogener Daten.

2. Auswirkungen in der Praxis

Die Standardvertragsklauseln sind in der Praxis insbesondere relevant, wenn Dienstleister*innen aus Drittländern, wie z.B. Microsoft, mit einer Datenverarbeitung beauftragt werden. Seit Wegfall des „EU-US Privacy Shield“ werden primär die Standardvertragsklauseln als Grundlage für den Datentransfer verwendet.

Die neuen Standardvertragsklauseln sind spätestens ab dem 27. September 2021 für neue Verträge zu verwenden. Bis zum 27. Dezember 2022 müssen die Unternehmen die bisherigen Standardvertragsklauseln durch die neuen ersetzt haben.

Entsprechend der Neuerungen habe ich in meiner Funktion als betriebliche Datenschutzbeauftragte die relevanten Fachbereiche über die überarbeiteten Standardvertragsklauseln informiert und den Inhalt dargelegt. Zudem habe ich eine Prüfung der Verträge veranlasst, die auf den bisherigen Standardvertragsklauseln beruhen, um einen etwaigen Anpassungsbedarf festzustellen. Die Bestandsaufnahme dauert noch an.

II. Telekommunikation-Telemedien-Datenschutz-Gesetz

Am 1. Dezember 2021 ist in Deutschland das „Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien“ (TTDSG) in Kraft getreten.

Das TTDSG ist neben der DSGVO und dem Bundesdatenschutzgesetz (BDSG) ein weiteres Bundesgesetz mit Datenschutzbestimmungen, speziell für den Bereich von Telekommunikations- und Telemediendiensten. Bislang waren die datenschutzrechtlichen Regelungen für Telekommunikations- und Telemediendienste im Telekommunikationsgesetz (TKG) und im Telemediengesetz (TMG) zu finden. Nunmehr sind sie im neuen TTDSG zusammengefasst.

Eine zentrale Regelung ist § 25 TTDSG. Sie betrifft die Einwilligungspflicht für Cookies und vergleichbare Technologien (zum Begriff „Cookies“ siehe Tätigkeitsbericht 2020 Buchstabe C Ziffer II. 1.).

Gemäß § 25 Abs.1 TTDSG ist „die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, nur zulässig, wenn der Endnutzer auf der Grundlage von klaren und umfassenden Informationen eingewilligt hat.“ Eine Endeinrichtung sind z.B. Smartphones, Tablets und Laptops.

Für den Einsatz von Cookies und vergleichbaren Technologien in Endeinrichtungen ist somit grundsätzlich eine Einwilligung der Nutzer*innen einzuholen, unabhängig davon, ob dabei personenbezogene Daten verarbeitet werden oder nicht. § 25 TTDSG bezweckt in erster Linie den Schutz der Privatsphäre bei Endeinrichtungen. § 25 Abs. 2 TTDSG sieht aber auch einige Ausnahmen von der Einwilligungspflicht vor, u.a. für die sog. technisch notwendigen Cookies, die zwingend erforderlich sind, um den jeweiligen Dienst zur Verfügung stellen zu können.

Ein solches Einwilligungserfordernis ist jedoch nicht neu. Bereits der EuGH und der BGH hatten in den Jahren 2019 und 2020 über die Einwilligungspflicht im Sinne einer aktiven Handlung (Opt-In-Verfahren) in Cookies entschieden (siehe Tätigkeitsbericht 2020 Buchstabe C, Ziffer II, Planet 49-Urteil).

Ausdrücklich gesetzlich geregelt wird dies aber nun erstmals in § 25 Abs. 1 TTDSG. Die Regelung setzt insoweit Art. 5 Abs. 3 ePrivacy-Richtlinie um. Bisher gab es keine europarechtskonforme Umsetzung dieser Richtlinien-Regelung.

III. Stand: Entwurf einer e-Privacy-Verordnung

Nach den ursprünglichen Plänen der Europäischen Kommission sollte zeitgleich mit der DSGVO die ePrivacy-Verordnung im Mai 2018 in Kraft treten und die derzeit geltende ePrivacy-Richtlinie (siehe Tätigkeitsbericht 2020, Buchstabe C. Ziffer III) ablösen.

Seitdem verzögert sich die Umsetzung. Der EU-Ministerrat hatte sich im Februar 2021 auf eine Version verständigt. Damit begannen die Trilog-Verhandlung zwischen den drei gesetzgebenden Institutionen der EU, namentlich der EU-Kommission, dem EU-Parlament und dem EU-Ministerrat. Allerdings bestehen unterschiedliche Positionen zwischen EU-Ministerrat und EU-Parlament, sodass bislang keine größeren Fortschritte erzielt werden konnten. Sollte die ePrivacy-Verordnung in Kraft treten, würde die Verordnung als höherrangiges Recht das TTDSG ablösen.

D. Datenschutz bei Radio Bremen

Im Berichtszeitraum habe ich in meiner Funktion als Aufsichtsbehörde im journalistisch-redaktionellen Bereich und als Datenschutzbeauftragte im administrativ-verwaltenden Bereich die Einhaltung der Datenschutzvorschriften bei Radio Bremen überwacht und zu vielfältigen datenschutzrechtlichen Anfragen aus den Fachbereichen und Redaktionen Stellung genommen. Aufgrund der Vielzahl an Anfragen, erläutere ich die datenschutzrechtliche Befassung an exemplarischen Einzelfällen.

I. Datenschutz in der Corona-Pandemie

Der Berichtszeitraum war geprägt von mehreren Gesetzesänderungen im Zusammenhang mit den Corona-Maßnahmen. Dabei stellten sich insbesondere im Beschäftigtendatenschutz wesentliche datenschutzrechtliche Fragestellungen.

1. Abfrage des Impf- und Genesenenstatus

Die bisherigen wissenschaftlichen Erkenntnisse deuten darauf hin, dass das Risiko sich selbst oder andere mit dem Corona-Virus anzustecken bei geimpften und genesenen Personen geringer ist. Im Arbeitskontext führt dies dazu, dass diese Personengruppe in bestimmten Bereichen flexibler eingesetzt werden kann im Vergleich zu Kolleg*innen, die einen solchen Status nicht haben. Auf Seite der Arbeitgeber*innen besteht daher ein Interesse, den Status in bestimmten Situationen abfragen zu dürfen, um Arbeitsabläufe besser planen zu können und ihrer arbeitsrechtlichen Fürsorgepflicht gegenüber den Mitarbeitenden nachzukommen.

Auch bei Radio Bremen stellte sich die Frage, ob Informationen über den Impf- oder Genesenenstatus einzelner Mitarbeiter*innen in bestimmten Fällen abgefragt werden dürfen.

Das war z.B. in dem Fall zu klären, dass die erforderlichen Abstände bei der Ausübung der dienstlichen Tätigkeit nicht eingehalten werden konnten oder an Drehorten, wo eine 2G-Zugangsregelung bestand.

Aus datenschutzrechtlicher Sicht ist die Abfrage des Impf- und Genesenenstatus nicht unproblematisch. Zum einen gab es zu diesem Zeitpunkt keine explizite gesetzliche Grundlage für die Abfrage dieser Daten. Ein allgemeines Fragerecht zum Impfstatus hatte der Gesetzgeber nur für bestimmte Bereiche gesetzlich vorgesehen, z.B. für Einrichtungen des Gesundheitsbereichs.

Zum anderen sind Daten zum Impf- und Genesenenstatus als Gesundheitsdaten im Sinne des Art. 4 Nr. 15 DSGVO zu qualifizieren und fallen damit in die besonderen Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO. Die Verarbeitung dieser sensiblen Daten ist grundsätzlich untersagt, es sei denn es liegt eine gesetzliche Ausnahme vor.

Im Rahmen des Beschäftigungsverhältnisses dürfen Gesundheitsdaten verarbeitet werden, wenn dies zur Erfüllung arbeitsrechtlicher Pflichten erforderlich ist und im Rahmen einer Abwägung das arbeitgeberseitige Interesse an der Verarbeitung das Interesse der Mitarbeitenden an der Geheimhaltung überwiegt. Im Rahmen dieser Abwägung sind verschiedene Aspekte zu berücksichtigen, z.B. die konkrete Tätigkeit der Person, der Kontakt zu Dritten, nicht alternativ ersetzbare Beiträge oder Zugangsbeschränkungen durch Dritte.

In bestimmten Einzelfällen habe ich die vorgenannten Voraussetzungen nach eingehender Prüfung als erfüllt angesehen. Dies ist dann der Fall, wenn die Kenntnis vom Impf- und Genesenenstatus für die Durchführung des Arbeitsverhältnisses und zum Schutz der Beschäftigten zwingend erforderlich ist. Dies gilt insbesondere in Situationen, in denen mangels Möglichkeit zur Einhaltung der Abstandsregeln ein hohes Infektionsrisiko besteht oder wenn die Abfrage für die Erfüllung der dem Arbeitgeber auferlegten Arbeitsschutzmaßnahmen notwendig ist.

Zudem habe ich die Möglichkeit der Abfrage in dem Fall bejaht, in dem durch Dritte 2G-Zugangsregelungen bestanden, z.B. bei der Berichterstattung von externen Veranstaltungen. In diesen Fällen werden Informationen zum Impf- oder Genesenenstatus benötigt, um gesetzlichen Nachweispflichten bei der Veranstaltung nachzukommen. Die Berichterstattung ist ein wesentlicher Teil des gesetzlichen Programmauftrags von Radio Bremen. In diesem Kernbereich ist es bei derartigen Veranstaltungen notwendig, den 2G-Status der Mitarbeitenden vor dem Einsatz geklärt zu haben, um die Berichterstattung sicherzustellen.

2. 3G-Regelung am Arbeitsplatz

Eine weitere Maßnahme der Pandemiebekämpfung ging mit der Änderung des Infektionsschutzgesetzes (IfSG) vom 22. November 2021 einher.

Mit dem neugefassten § 28b IfSG hat der Gesetzgeber erstmals eine 3G-Zugangsregelung am Arbeitsplatz eingeführt. Seitdem gilt, dass in Arbeitsstätten mit physischen Kontakten zwischen Arbeitgeber*innen und Beschäftigten untereinander oder zu Dritten gem. § 28b Abs. 1 S. 1 IfSG ausschließlich Beschäftigte mit einem 3G-Status (geimpft, genesen, getestet) die Arbeitsstätte betreten dürfen.

Den Arbeitgeber trifft hierbei gem. § 28b Abs.3 IfSG eine Kontrollpflicht, die Einhaltung dieser Regelung zu dokumentieren. Die Vorschrift gilt zunächst bis zum 19. März 2022.

Aufgrund dieser gesetzlichen Vorgaben hat Radio Bremen ein zentrales Überprüfungsverfahren eingeführt, in welches ich im Vorfeld vor Umsetzung der Maßnahme eingebunden war. Das Überprüfungsverfahren von Radio Bremen entspricht den datenschutzrechtlichen Bestimmungen.

Es werden nur die Daten erhoben, die erforderlich sind, um den gesetzlichen Verpflichtungen der Kontrolle und Dokumentation des 3G-Status nachzukommen. Die Nachweislisten werden vertraulich und geschützt vor unberechtigten Zugriffen und nur für die Dauer der Zweckerreichung geführt.

Das Überprüfungsverfahren führte bei einigen Kolleg*innen zu Nachfragen. Es bestand die Sorge, dass dem Arbeitgeber ein umfangreiches Fragerecht eingeräumt werde.

Die entsprechenden Anfragen der Kolleg*innen konnte ich jedoch verneinen, da die Regelung kein Auskunfts- und Fragerecht der Arbeitgeber*innen über den Impf- und Genesenenstatus der Mitarbeitenden mit sich bringt.

Zwar müssen Arbeitgeber*innen von ihren Mitarbeitenden einen entsprechenden Nachweis verlangen, es bleibt aber ihnen selbst überlassen, welchen 3G-Nachweis sie dabei vorlegen.

Insbesondere können auch geimpfte und genesene Personen statt eines Impfnachweises einen tagesaktuellen Testnachweis erbringen, sodass die Arbeitgeber*innen keine Kenntnis von der Impfung oder einer Corona-Erkrankung erhalten müssen.

3. Weitere Beratung im Zusammenhang mit Corona-Maßnahmen

Aufgrund der anhaltenden Corona-Situation waren bei Radio Bremen Veranstaltungen mit Publikum nur eingeschränkt möglich.

Im Zusammenhang mit den stattfindenden Veranstaltungen war ich beratend tätig. Es galt das 3G-Konzept (Zutritt nur für geimpfte, genesene und getestete Personen) und die gesetzlich vorgesehene Erhebung von Daten zur Kontaktnachverfolgung gemäß der 28. Verordnung zum Schutz vor Neuinfektionen mit dem Corona-Virus SARS-CoV-2 Bremen datenschutzkonform in die Praxis umzusetzen.

II. Datenschutz im Programmbereich

1. Kontaktdatenbank für die redaktionelle Einbindung von Expert*innen

Im Berichtszeitraum waren die Planungen zu der Einführung einer Kontaktdatenbank für die redaktionelle Einbindung von Expert*innen abgeschlossen und die neue Datenbank konnte nach zwei Jahren intensiver Projektarbeit an den Start gehen.

Die bisherige PlanPoint-Datenbank wurde infolgedessen abgelöst. Die neue Kontaktdatenbank soll den Redakteur*innen die Suche nach geeigneten Interviewgästen erleichtern und durch die Vielfalt der Expert*innen für mehr Diversität in die Programme von Radio Bremen sorgen. Neben technischen und IT-sicherheitsrelevanten Herausforderungen spielte der Datenschutz eine zentrale Rolle bei der Umsetzung der Kontaktdatenbank (siehe Tätigkeitsbericht 2020, Buchstabe D, Ziffer II 2).

2. Beanstandungen durch die Datenschutzbeauftragte

Im Berichtszeitraum musste ich keine förmlichen Beanstandungen gegenüber Radio Bremen aussprechen. Gesonderte Kontrollmaßnahmen waren im journalistisch-redaktionellen Bereich ebenfalls nicht erforderlich. Da ich als Mitarbeiterin im Justizariat auch für die äußerungsrechtlichen Angelegenheiten innerhalb des Justiziariats zuständig bin, ist sichergestellt, dass ich als Datenschutzbeauftragte von solchen Vorgängen Kenntnis erlange.

III. Datenschutz im Verwaltungsbereich

1. Einführung von Microsoft 365

a. Allgemeines

Die Corona-Pandemie hat gezeigt, dass digitale Lösungen essentiell für eine funktionierende Zusammenarbeit in der Arbeitswelt sind. Im Zuge der Pandemie arbeiten viele Beschäftigte im Homeoffice oder mobil. Zusammenkünfte finden nicht mehr analog sondern virtuell statt. Videokonferenzen erlangten dabei eine zentrale Bedeutung für die dienstliche Kommunikation. Dies prägte und prägt weiterhin den Arbeitsalltag bei Radio Bremen.

Dies unterschiedlichen Arbeitsformen haben sich neben der Erbringung der Arbeitsleistung in Präsenz inzwischen bei Radio Bremen etabliert, sodass davon auszugehen ist, dass das Arbeiten aus dem Homeoffice und die mobile Arbeit auch über die Pandemie hinaus für die Mitarbeitenden von Interesse sein und Bestand haben werden.

Doch auch Radio Bremen verfolgt im Rahmen ihrer Unternehmensstrategie u.a. das Ziel der „Digitalisierung und Flexibilität“. Auf dieser Basis und im Rahmen von „New Work“ soll das Arbeiten in Home und Mobile Office bei Radio Bremen zukunftsfähig gemacht werden.

Der Einsatz und die Nutzung von digitalen Kollaborationsplattformen ist dafür unerlässlich. Einen ersten Schritt in diese Richtung geht Radio Bremen nun mit der Einführung von Microsoft 365 (M365), einem Produktpaket mit unterschiedlichen Web- und Onlinediensten.

Die wohl bekannteste Anwendung ist Microsoft Teams (MS Teams): Diese Plattform ermöglicht die direkte Videotelefonie, einen schnelleren Informationsaustausch über die Chat-Funktion sowie die gemeinsame Projektarbeit und Terminplanung.

Als Videokonferenzsystem hat sich MS Teams inzwischen in den meisten Rundfunkanstalten etabliert. Mitarbeitende Radio Bremens können an diesen Konferenzen bislang nur „passiv“ auf Einladung Dritter im Rahmen einer Gastnutzung und ohne weitergehende Nutzungsmöglichkeiten der Funktionen teilnehmen.

b. Arbeitsgruppe

Im März 2021 ist das Projekt „Einführung von M365“ an den Start gegangen. Dazu hat sich eine Arbeitsgruppe gebildet, bestehend aus Kolleg*innen der Personalabteilung, der IT, dem Personalrat sowie dem IT-Sicherheitsbeauftragten und der Datenschutzbeauftragten. Die Arbeitsgruppe wurde von einem externen IT-Dienstleister unterstützt, der Unternehmen bei der Einführung von M365 fachlich berät und begleitet.

Die Arbeitsgruppe hat mehr als ein halbes Jahr intensiv an einer ersten Einführungsphase von M365 gearbeitet. Im Fokus der ersten Einführungsphase standen die für den grundlegenden Betrieb von Microsoft 365 benötigten Dienste.

c. Datenschutz und IT-Sicherheit

Die Einführung von M365 bzw. einzelner Dienste ist ein umfangreiches und komplexes Vorhaben, bei dem insbesondere das Datenschutzrecht, die IT,- und Informationssicherheit eine zentrale Rolle spielen.

Erfreulich ist, dass im Kollegium der Datenschutz von Anfang an als eine sehr wichtige Säule für die sichere Einführung von M365 verstanden wurde und auf dieser Basis eine erfolgreiche und pragmatische Zusammenarbeit stattgefunden hat.

Die Wichtigkeit des Datenschutzes und der IT-Sicherheit ist insbesondere darauf zurückzuführen, dass die einzelnen Dienste von M365 „cloudbasiert“ funktionieren.

Das heißt, dass die bei der Nutzung der Dienste zu verarbeitenden Daten von der jeweiligen Endeinrichtung (Computer, Tablet, Smartphone) über das Internet auf den Server bzw. die Rechenzentren des Cloud-Anbieters übertragen und dort gespeichert werden. Dabei kann dieser Server überall auf der Welt stehen.

Für Microsoft-Kunden mit Sitz in Deutschland werden die Daten zwar automatisch in deutschen Rechenzentren von Microsoft gespeichert. Problematisch ist jedoch, dass die verschiedenen US-Sicherheitsgesetze wie der „Patriot Act“ und der „Cloud Act“ den Zugriff amerikanischer Sicherheitsbehörden auf den Datenbestand von US-Unternehmen ermöglichen, unabhängig davon, ob die Daten auf Unternehmensservern innerhalb oder außerhalb der USA gespeichert werden. Die Cloudnutzung führt also dazu, dass eine Datenübertragung in die USA erfolgen kann.

Als Verantwortliche einer Datenverarbeitung hat Radio Bremen dafür Sorge zu tragen, dass interne vertrauliche und streng vertrauliche Daten und Informationen der Rundfunkanstalt und der Mitarbeitenden vor dem Zugriff von Dritten geschützt sind. Radio Bremen verfügt über eine Vielzahl von Daten und Informationen, die es zu schützen gilt. Hierbei kann es sich zum Beispiel um Geschäftsgeheimnisse oder besondere personenbezogene Daten im Sinne von Art. 9 DSGVO handeln, an deren Geheimhaltung ein hohes schutzwürdiges Interesse besteht. Im Bereich der journalistisch-redaktionellen Datenverarbeitung in der Cloud, muss ein besonderer Fokus darauf liegen, dass das Redaktionsgeheimnis und der Informant*innenschutz gewahrt bleiben.

Vor diesem Hintergrund hat die Arbeitsgruppe ein Sicherheitskonzept mit umfangreichen technischen und organisatorischen Maßnahmen erarbeitet, um den Datenschutz und die IT-Sicherheit bei der Anwendung der M365-Dienste insbesondere in Bezug auf den Informant*innenschutz und die Sicherung des Redaktionsgeheimnisses zu gewährleisten.

Eine zentrale organisatorische Maßnahme ist die sogenannte Datenklassifizierung. Hierbei handelt es sich um eine ARD-weit abgestimmte Übersicht, in der der Schutzbedarf der jeweiligen Daten und Informationen, die in der elektronischen Arbeitsumgebung entstehen, definiert ist. Auf Basis dieser Angaben wird Radio Bremen festlegen, welche Daten in einer Cloudumgebung verarbeitet werden dürfen und welche nicht. Alle Mitarbeitenden werden darüber vor Einführung von M365 umfassend informiert und zudem durch Schulungs- und andere geeignete Maßnahmen unterstützt werden.

Eine wichtige technische Schutzmaßnahme, die im Zuge der Einführung von M365 umgesetzt wird, ist die Multi-Faktor-Authentifizierung. Dabei wird der jeweilige Benutzer*innen-Account nicht nur durch den Benutzernamen und das dazugehörige Passwort gesichert, sondern durch weitere Faktoren, wie z.B. die Bestätigung des Logins per Telefon oder Smartphone-App. Diese erweiterte Sicherheitsstufe macht den Account sicherer vor unberechtigten Zugriffen.

Um sich als unbefugte Person im System anzumelden, reicht es nicht aus, in den Besitz der Anmeldedaten (Benutzername und Passwort) zu gelangen, sondern es müsste der zusätzliche Faktor wie etwa das dienstliche Smartphone der Nutzer*innen vorhanden sein.

Aus datenschutzrechtlicher Sicht ist festzuhalten, dass über die geplanten technischen und organisatorischen Maßnahmen eine Basis geschaffen wird, auf welcher eine DSGVO-konforme Nutzung der einzuführenden Dienste möglich wird.

d. Änderungen von IT-Regelungen zur Ermöglichung der Nutzung von Cloud-Diensten

Bislang gab es keine Regelung bei Radio Bremen, welche die Datenablage in Cloudsystemen bei externen Dienstleister*innen regelt. Daher war eine Erweiterung der bereits bestehenden IT-Regelungen auf Cloud-Dienste erforderlich. Die aktualisierten IT-Regelungen werden noch vor der Einführung von M365 in Kraft treten.

e. Weitere Schritte

Radio Bremen wird die für den grundlegenden Betrieb von M365 benötigten Dienste zum Jahresbeginn 2022 einführen. Darüber hinaus ist geplant, den Anwendungsumfang von M365 zu einem späteren Zeitpunkt durch die Bereitstellung weiterer Dienste zu erweitern. Dieses Vorhaben wird zukünftig in einer gesonderten Projektgruppe beraten, in die ich in meiner Funktion als Datenschutzbeauftragte eingebunden sein werde.

Die bei Radio Bremen aktuell genutzte Videokonferenz-Software „Jitsi Meet“ wird zunächst weiter genutzt werden. Alle Videokonferenztermine werden aber schrittweise Anfang 2022 auf MS Teams umgestellt werden.

2. Datenschutzrechtliche Schulungen der Mitarbeitenden

Im Berichtszeitraum haben der Datenschutzbeauftragte der Bremedia Produktion GmbH und ich insgesamt 100 Mitarbeitende datenschutzrechtlich geschult. Datenschutzrechtliche Schulungen sind für alle Mitarbeitenden von Radio Bremen verpflichtend.

Der Rundfunkbetrieb basiert auf zahlreichen IT-gestützten Systemen und Anwendungen. Viele Arbeitsprozesse werden elektronisch gesteuert. Gleichzeitig ist es in Zeiten der Pandemie erforderlich, auch mittels mobiler Geräte auf dienstliche Daten zuzugreifen.

Diese Arbeitsweisen beinhalten verschiedene Risiken für den Datenschutz und die IT-Sicherheit. Unberechtigte Dritte können sich unter Umständen Zugang zu unseren IT-Systemen verschaffen und die Sende- und Produktionssicherheit gefährden oder auf die Daten und Informationen von Radio Bremen zugreifen.

Ziel der Schulungen ist es daher, die Mitarbeitenden mit den besonderen Erfordernissen des Datenschutzes vertraut zu machen und für die bestehenden Gefahren, die mit der Nutzung der bei uns eingesetzten IT-Systeme einhergehen, zu sensibilisieren. Dies gilt sowohl für den Schutz personenbezogener Daten als auch für die IT-Sicherheit.

Schwerpunkte der Schulungen waren die Vermittlung der datenschutzrechtlichen Grundlagen und Kenntnisse zum Datenschutz am Arbeitsplatz. Dazu gehören die Regelungen zum Schutz der personenbezogenen Daten, die bestehenden Rechte der Betroffenen, die Besonderheiten beim Verarbeiten von Daten in einer öffentlich-rechtlichen Rundfunkanstalt (Medienprivileg), die Aufgaben der Datenschutzbeauftragten, die technisch-organisatorischen Maßnahmen zum Schutz von Daten sowie die rechtlichen Folgen von Verstößen.

Ein wichtiger Faktor beim Schutz sensibler Daten und Informationen ist die Anmeldung der Benutzer*innen an den IT-Systemen eines Unternehmens. In diesem Zusammenhang spielt die Passwortsicherheit eine zentrale Rolle. Diese wurde im Rahmen der Schulung ebenfalls erläutert und Möglichkeiten aufgezeigt, ein individuelles und sicheres Passwort für das eigene Benutzerkonto zu erstellen.

3. ARD-Mindeststandard zur Authentisierung von ARD und Deutschlandradio

Zukünftig wird es eine Erhöhung der Passwortsicherheit von Benutzer*innen-Konten durch erweiterte und angepasste Vorgaben und Maßnahmen geben.

ARD und Deutschlandradio haben sich auf einen Mindeststandard für den Umgang mit Benutzer*innen-Konten und Authentisierungsinformationen verständigt, um für mehr Sicherheit für die Benutzer*innen-Konten zu sorgen.

Die Anforderungen an die Passwortsicherheit sowie die Maßnahme der Multi-Faktor-Authentifizierung wurden bereits im Zusammenhang mit der Einführung von Microsoft Teams berücksichtigt und umgesetzt.

4. SAP-Prozessharmonisierung „(D)ein SAP“

Das ARD-Strukturprojekt „(D)ein SAP“ wurde im Berichtsjahr von den Datenschutzbeauftragten der einzelnen Rundfunkanstalten weiterhin intensiv begleitet (siehe Tätigkeitsbericht Buchstabe D, Ziffer II 3).

Als Datenschutzbeauftragte bin ich auf zwei Ebenen in das Projekt eingebunden: als Mitglied des „Arbeitskreis der Datenschutzbeauftragten der ARD, des ZDF und des Deutschlandradios“ (AKDSB) und als Mitglied der internen Radio Bremen Projektgruppe, die an der Umsetzung der Einzelprojekte von (D)einSAP bei Radio Bremen arbeitet.

In den regelmäßig stattfindenden Projektsitzungen werden die anstehenden Veränderungen bzw. Umstellungen auf das SAP-System bei Radio Bremen beraten.

5. Arbeitsgruppe IT-Sicherheit

Die Arbeitsgruppe IT-Sicherheit hat im Berichtszeitraum wieder quartalsweise getagt. In ihr sind neben Vertretern aus der Koordination Technik

und dem IT-Bereich, eine Vertreterin der Programmdirektion, der IT-Sicherheitsbeauftragte, der Datenschutzbeauftragte der Bremedia Produktion GmbH sowie ich als Datenschutzbeauftragte von Radio Bremen vertreten.

Ziel der Arbeitsgruppe ist der bereichsübergreifende Informationsaustausch und die Abstimmung zu grundsätzlichen und aktuellen Themen des Datenschutzes und der IT-Sicherheit innerhalb der Unternehmensgruppe. Ein Schwerpunktthema war im Berichtszeitraum die Einführung von M365 bzw. der sonstige Einsatz von Cloud-Systemen.

6. Datenschutzvorfälle

Positiv ist, dass im Berichtszeitraum keine Datenschutzvorfälle bei Radio Bremen vorkamen. Infolgedessen war eine Meldung gemäß Art. 33 DSGVO an die Landesbeauftragte für Datenschutz und Informationsfreiheit Bremen nicht erforderlich.

E. Auskunftsanfragen und Beschwerden

Auskunftsanfragen erreichen Radio Bremen in der Regel als allgemeine datenschutzrechtliche Auskunftsanfrage von Rundfunkteilnehmer*innen auf Basis von Art. 15 DSGVO. Förmliche Auskunftersuchen aus dem Haus von festen oder freien Mitarbeiter*innen habe ich im Berichtszeitraum nicht erhalten.

Zudem erreichte mich eine überschaubare Anzahl an Beschwerden, die sich auf die Berichterstattung von Radio Bremen bezogen.

I. Auskunftsanfragen gemäß Art. 15 DSGVO

Das datenschutzrechtliche Auskunftsrecht gewährleistet ein wichtiges Betroffenenrecht. Nach Art. 15 Abs.1 DSGVO haben betroffene Personen das Recht, von Verantwortlichen einer Datenverarbeitung eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Ist das der Fall, haben die betroffenen Personen ein Recht auf Auskunft über diese Daten und darüberhinausgehende Informationen zu deren Verarbeitung.

Auskunftsanfragen der im Bundesland Bremen wohnhaften Rundfunkteilnehmer*innen werden von der Stelle beantwortet, an die die Anfrage gerichtet wird. Dies können entweder der Zentrale Beitragsservice von ARD, ZDF und Deutschlandradio (ZBS) sein oder Radio Bremen selbst.

Im Berichtsjahr hat der ZBS für Radio Bremen insgesamt 51 Datenauskünfte antragsgemäß erteilt. Bei der Datenschutzbeauftragten von Radio Bremen gingen insgesamt fünf Auskunftersuchen ein, die antragsgemäß beantwortet wurden. In den meisten Fällen beehrten die Anfragenden Auskünfte über die zu ihrer Person gespeicherten Daten.

II. Beschwerden

Weiterhin gab es einige Beschwerden von in der Berichterstattung abgebildeten Personen, die nachträglich aus dem veröffentlichten Material gelöscht werden wollten, da sie sich in ihrem Persönlichkeitsrecht verletzt sahen, obwohl sie zuvor eine Einwilligung in die Aufnahmen erteilt hatten.

Bei Fotografien oder Bewegtbildern mit erkennbaren Personen handelt es sich um personenbezogene Daten i.S.d. Art. 4 Nr. 1 DSGVO, die digital verarbeitet werden.

Soweit Bilder im journalistischen Bereich veröffentlicht werden, ist jedoch nicht die DSGVO, sondern das Kunsturhebergesetz (KUG) maßgeblich. Als EU-Recht hätte die DSGVO grundsätzlich Vorrang vor dem nationalen Recht bzw. dem KUG. Gemäß Art. 85 Abs. 2 DSGVO dürfen die Mitgliedsstaaten für die Datenverarbeitung zu journalistischen Zwecken oder zu wissenschaftlichen, künstlerischen oder literarischen Zwecken Abweichungen oder Ausnahmen von den Grundsätzen der Verarbeitung nach der DSGVO vorsehen.

Nach Auffassung des Bundesgerichtshofs bilden die §§ 22 und 23 KUG solche abweichenden nationalen Regelungen, die von der Öffnungsklausel gedeckt sind. Das Recht am eigenen Bild ist eine besondere Ausprägung des allgemeinen Persönlichkeitsrechts und in § 22 KUG geregelt.

Die eingangs genannten Fälle werden daher nicht nach der DSGVO sondern nach dem KUG beurteilt, sodass die Beantwortung nicht in den Zuständigkeitsbereich der Datenschutzbeauftragten fällt. Daher habe ich diese Beschwerden an die zuständigen Kolleg*innen im Justizariat weitergegeben.

F. Zusammenarbeit

Als Datenschutzbeauftragte von Radio Bremen arbeite ich mit den Aufsichtsbehörden und den betrieblichen Datenschutzbeauftragten im öffentlich-rechtlichen Rundfunk kontinuierlich zusammen.

I. Rundfunkdatenschutzkonferenz

Die Rundfunkdatenschutzkonferenz (RDSK) besteht aus den unabhängigen Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten, die Aufsichtsfunktionen nach Art. 51 ff. DSGVO wahrnehmen.

Als Aufsichtsbehörde über die Datenverarbeitung im journalistisch-redaktionellen Bereich gemäß § 14 BremAGDSGVO bin ich ebenfalls Mitglied der RDSK.

Die Erforderlichkeit der Zusammenarbeit ist zum einen rechtlich geboten und zum anderen deshalb sinnvoll, weil die einzelnen Rundfunkanstalten auf verschiedenen Ebene miteinander vernetzt sind und eng zusammenarbeiten. Dies betrifft zum Beispiel das Programm, die Verwaltung, die IT und die Produktion. Viele Vorgänge und Projekte betreffen daher von vornherein mehrere oder alle Rundfunkanstalten in gleicher Weise. Über alle grundsätzlichen Fragen des Datenschutzes, die in diesem Zusammenhang auftreten, stimmen sich die Datenschutzaufsichten in der RDSK ab.

In der Geschäftsordnung der RDSK sind deren Aufgaben und Arbeitsweisen festgelegt. Eine zentrale Aufgabe ist die Förderung der einheitlichen Anwendung und Auslegung datenschutzrechtlicher Regelungen im öffentlich-rechtlichen Rundfunk.

In diesem Zusammenhang erarbeitet die RDSK Stellungnahmen, Orientierungshilfen, und Positionspapiere zu inhaltlichen, technischen oder organisatorischen Fragen des Datenschutzes, die sie auf ihrer Webseite

<https://www.rundfunkdatenschutzkonferenz.de>

publiziert.

Im Berichtszeitraum fanden zwei Videokonferenzen der RDSK statt. Themen waren u.a. das TTDSG, die Nutzung von Drittplattformen durch die Rundfunkanstalten, der Einsatz der Luca-App sowie die Anwendung von Art. 83 DSGVO (Verhängung von Bußgeldern).

Aus gegebenem Anlass veröffentlichte die RDSK im Berichtszeitraum das Positionspapier „Datenschutzrechtliche Eckpunkte zum Einsatz von Kollaborationssystemen“. Darin sind die datenschutzrechtlichen Anforderungen formuliert, die bei dem Einsatz und der Nutzung dieser Kommunikationsplattformen umzusetzen sind.

II. Arbeitskreis der Datenschutzbeauftragten

Die Mitglieder der RDSK stehen im regelmäßigen Kontakt zu den betrieblich bestellten Datenschutzbeauftragten im öffentlich-rechtlichen Rundfunk. Der Austausch erfolgt im AKDSB, dem ich als betriebliche Datenschutzbeauftragte ebenfalls angehöre.

Der Arbeitskreis dient dem datenschutzrechtlichen Meinungs- und Erfahrungsaustausch sowie der Förderung eines gemeinsamen Verständnisses datenschutzrechtlicher Rahmenbedingungen in den Rundfunkanstalten.

Im Unterschied zur RDSK fungiert der AKDSB auf operativer Ebene und berät dort in datenschutzrelevanten Angelegenheiten.

Darüber hinaus koordiniert der AKDSB den Datenschutz beim Rundfunkbeitragseinzug und bei Gemeinschaftsprojekten. Aktuelle Fragen und Themen bezüglich des Rundfunkteilnehmerdatenschutzes werden regelmäßig im AKDSB erörtert.

Es besteht daher eine enge Zusammenarbeit mit den betrieblichen Datenschutzbeauftragten des ZBS, die ebenfalls Mitglieder des Arbeitskreises sind. Auch der Datenschutzbeauftragte von ARTE und der Datenschutzbeauftragte des Österreichischen Rundfunks (ORF) nehmen als Mitglieder regelmäßig an den Sitzungen teil.

Im Berichtszeitraum fanden mehrere Sitzungen des AKDSB per Videokonferenz statt.

Der Arbeitskreis ist zudem um neue Mitglieder erweitert worden. Fortan nehmen die Datenschutzbeauftragten der Schweizerischen Radio- und Fernsehgesellschaft (SRG SSR) an seinen Sitzungen teil. Im Berichtszeitraum fand bereits ein erster Austausch mit den neuen Kolleg*innen statt. Themen waren unter anderem die Organisation des Datenschutzes im öffentlich-rechtlichen Rundfunk in Deutschland, Österreich und der Schweiz und der Datenschutz im investigativen Journalismus.

Die thematischen Schwerpunkte im AKDSB bildeten im Berichtszeitraum insbesondere die neuen Standardvertragsklauseln der EU-Kommission, die datenschutzrechtliche Befassung mit Einzelprojekten des Harmonisierungsprojekts (D)ein SAP, der Einsatz von Nutzungsmessungsverfahren in Telemedienangeboten und die Überarbeitung der Social Media Guidelines (datenschutzrechtliche Handlungsanweisungen für Telemedienangebote).

III. Datenschutzkonferenz

Im Berichtszeitraum fanden zwei gemeinsame Termine der Datenschutzkonferenz (DSK) mit den spezifischen Aufsichtsbehörden statt.

Die DSK besteht aus den unabhängigen Datenschutzbehörden des Bundes und der Länder. Zu den spezifischen Aufsichtsbehörden gehören die Datenschutzbeauftragten der Rundfunkanstalten und die der Kirchen.

Auf der Tagesordnung standen u.a. aktuelle Entwicklungen im Datenschutzrecht, Kollaborationssysteme, das TTDSG und der Einsatz der Luca-App durch öffentliche Stellen.

IV. IVZ-Jahrestreffen

Das Informationsverarbeitungszentrum (IVZ) ist eine Gemeinschaftseinrichtung der ARD, des DLR und der Deutschen Welle (DW) unter der Federführung des Rundfunk Berlin-Brandenburg (rbb).

Das IVZ hat primär die Aufgabe, die Vereinheitlichung von IT-Prozessen innerhalb der Rundfunkanstalten zu unterstützen. Die Rechtsgrundlage der IVZ-Kooperation bildet die IVZ-Verwaltungsvereinbarung. Im Rahmen der vorgenannten Aufgabenwahrnehmung werden im IVZ diverse Datenverarbeitungen durchgeführt.

Die an der Gemeinschaftseinrichtung beteiligten Rundfunkanstalten sind für die Datenverarbeitung beim IVZ gemäß Art. 26 DSGVO gemeinsam verantwortlich und für die Kontrolle über die Einhaltung der datenschutzrechtlichen Bestimmungen beim IVZ zuständig. In Ergänzung zu der IVZ-Verwaltungsvereinbarung besteht daher eine Vereinbarung zur gemeinsamen Verantwortlichkeit bei der Verarbeitung von personenbezogenen Daten (Joint-Controller-Agreement).

Auch im Berichtszeitraum fand das jährliche Treffen zwischen der Geschäftsführung und den zuständigen Mitarbeitenden des IVZ und den Datenschutzbeauftragten der Rundfunkanstalten per Videokonferenz statt.

In diesem Rahmen haben sich die Mitglieder über Maßnahmen zur weiteren Verbesserung des Austausches zwischen dem IVZ und den Datenschutzbeauftragten verständigt. Es wurde u.a. eine stärkere Einbeziehung des Datenschutzbeauftragten des IVZ verabredet.

G. Fortbildungen

Zur Erhaltung und Erweiterung meines datenschutzrechtlichen Fachwissens habe ich im vergangenen Jahr an zwei Fortbildungen teilgenommen

Das Webinar „Cloud Computing“ vermittelte neben dem technischen Basiswissen zu Cloud-Anwendungen allgemein den datenschutzkonformen Umgang beim Einsatz eines Cloud-Systems im Unternehmen. Das in diesem Rahmen erlangte Fachwissen habe ich dann in dem Seminar „Microsoft 365 - Sicherheit und Compliance: Worauf Sie bei Einführung und Betrieb achten sollten“ vertieft. Hier wurden die Themen Datenschutz, Sicherheit, Compliance und Datenschutz explizit beim Einsatz von M365 behandelt.

Das auf Basis der Fortbildungen erlangte Fachwissen war sehr hilfreich in der datenschutzrechtlichen Beratung bei der Einführung von M365 bei Radio Bremen. Dieses konnte ich direkt in die Arbeitsgruppe transferieren, sodass wichtige Aspekte von vornherein berücksichtigt und umgesetzt werden konnten.

Bremen, 16. März 2022

Gezeichnet

Ivka Jurčević