TÄTIGKEITSBERICHT

DES DATENSCHUTZBEAUFTRAGTEN
DES NORDDEUTSCHEN RUNDFUNKS
HORST BRENDEL

FÜR DEN ZEITRAUM

01. JANUAR 2015 BIS 31. DEZEMBER 2015

dem Verwaltungsrat des NDR vorgelegt gemäß
§ 41 Abs. 9 des Staatsvertrages über den
Norddeutschen Rundfunk

Danksagung

Mein besonderer Dank gilt auch in diesem Jahr **Frau Marlies Mein** für ihren Einsatz und ihre Unterstützung bei der Erledigung der Aufgaben des Datenschutzbeauftragten, insbesondere bei der Erstellung dieses Tätigkeitsberichts. Ihr engagiertes und zuverlässiges Mitwirken verdient in jeder Form Anerkennung.

Herzlich danken möchte ich außerdem **Frau Cornelia Weitzel-Kerber**, die mich bei der Wahrnehmung meiner Aufgaben im AK DSB und im NDR unterstützt und ergänzt hat.

GLIEDERUNG

TEIL A - BERICHT

TEIL B - ANLAGEN

Anlage 1	Stellungnahme von ARD, BDZV, DJV, Deutscher Presserat, VDZ, ver.di, VPRT und ZDF zum Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten
Anlage 2	Gerichtsentscheidungen mit datenschutzrechtlichem Schwerpunkt 2015
Anlage 3	Stellungnahme des Arbeitskreises der Rundfunkbeauftragten für den Datenschutz zur Evaluation der Datenschutzbestimmungen im Rundfunkbeitragsstaatsvertrag
Anlage 4	Chronologische Aufstellung der Projekte und Vorhaben zur Verarbeitung personenbezogener Daten im NDR in 2015
Anlage 5	Zusammenfassung der Beschwerden von Rundfunkteilnehmern
Anlage 6	Arbeitskreis der Rundfunkdatenschutzbeauftragten / Wesentliche Themenschwerpunkte in den Sitzungen im Jahr 2015

ANHANG

Anhang 1	Position, Aufgaben und Befugnisse des NDR Datenschutzbeauftragten
Anhang 2	Verfahrenskodex der Rundfunkbeauftragten für den Datenschutz zur Behandlung von Eingaben oder Hinweisen Dritter
Anhang 3	Wortlaut des Art. 28 EG-Datenschutzrichtlinie

A. Zusammenfassung der wesentlichen Ereignisse und Ergebnisse im Berichtszeitraum

- Im Jahr 2015 gab es für den Datenschutzbeauftragten keinen Anlass, eine förmliche Beanstandung auszusprechen.
- Die Anzahl der im Rahmen der Vorabprüfung zu begutachtenden Projekte und Vorhaben zur Verarbeitung personenbezogener Daten war mit 23 Projekten geringfügig größer als die Anzahl der im Vorjahr geprüften, bewegte sich aber im durchschnittlichen Mittel der letzten Jahre (siehe E. III.).
- Die Anzahl der an den Datenschutzbeauftragten gerichteten Eingaben hat sich 2015 im Rahmen der üblichen Schwankungsbreite gehalten (siehe E. VI.).
- Der NDR Datenschutzbeauftragte bzw. die Stellvertretende NDR Datenschutzbeauftragte beteiligten sich wie in den Vorjahren am Treffen der Datenschutzbeauftragten beim Informations-Verarbeitungszentrums (IVZ) in Berlin sowie an der Prüfung der Beihilfe- und Bezüge-Zentrum GmbH (bbz) in Bad Dürkheim.

B. Rechtsgrundlagen der Tätigkeit des NDR Datenschutzbeauftragten

Die Rechtsvorschriften für die Tätigkeit des Datenschutzbeauftragten haben sich im Berichtszeitraum nicht verändert. Als **Anhang 1** ist eine Darstellung der wesentlichen einschlägigen rechtlichen Bestimmungen beigefügt.

Mit Eingaben und Hinweisen Dritter verfährt der Datenschutzbeauftragte gemäß dem vom Arbeitskreis der Rundfunkbeauftragten für den Datenschutz (AK DSB) 2006 beschlossenen „Verhaltenskodex der Rundfunkbeauftragten für den Datenschutz zur Behandlung von Eingaben und Hinweisen Dritter"; dieser ist als **Anhang 2** beigefügt.

Der Datenschutzbeauftragte ist eine datenschutzrechtliche Kontrollstelle im Sinne von Art. 28 EG-Datenschutzrichtlinie, deren Text als **Anhang 3** beigefügt ist.

C. Personalien

Der Datenschutzbeauftragte des NDR, Horst Brendel, wurde vom Verwaltungsrat des NDR für die Dauer von fünf Jahren – **vom 1. Dezember 2011 bis zum 30. November 2016** – bestellt.

Der Datenschutzbeauftragte nimmt seine **Aufgabe nebenamtlich** zu seiner Tätigkeit als Leiter der Rechtsabteilung und Stellvertretender Justitiar des NDR wahr.

Durch Beschluss vom 26. März 2013 bestellte der Verwaltungsrat **Frau Cornelia Weitzel-Kerber** für die Zeit vom 24. Juni 2014 bis zum 30. November 2016 zur **Stellvertretenden Datenschutzbeauftragten**. Frau Weitzel-Kerber nimmt diese Aufgabe ebenfalls nebenamtlich zu ihrer Tätigkeit als Referentin im Justitiariat des NDR wahr.

Soweit der Datenschutzbeauftragte in personellen Angelegenheiten als Arbeitsrechtsexperte im Justitiariat tätig wird, werden dabei auftretende datenschutzrechtliche Fragestellungen von Frau Weitzel-Kerber bearbeitet.

Das Thema Datensicherheit wird im NDR von **Herrn Karl-Jürgen Hanßmann** betreut, der in der Hauptabteilung Informations-, Medien- und Verbreitungstechnik beschäftigt ist.

D. Wesentliche rechtliche Entwicklungen im Berichtszeitraum

I. Gesetzgebung

Europäische Datenschutz-Grundverordnung

Am 25. Januar 2012 hatte die Kommission den Entwurf für eine Datenschutz-Grundverordnung vorgelegt, die die aus dem Jahr 1995 stammende Richtlinie 95/46/EG ablösen und das Datenschutzrecht für alle Mitgliedsstaaten verbindlich regeln soll. Ein unter der irischen Präsidentschaft vorgelegter Entwurf scheiterte im Juni 2013 im Rat. Nach langen Verhandlungen nahm der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) den wesentlich vom Abgeordneten der Grünen Jan Philipp Albrecht mitgestalteten Kompromissvorschlag am 21. Oktober 2013 mit großer Mehrheit an. Am 12. März 2014 bestätigte das Europaparlament diese Entscheidung.

In den sich anschließenden Beratungen im Rat wurden zahlreiche Änderungsvorschläge diskutiert. Am 24. Juni 2015 begannen die Beratungen zwischen der Kommission, Vertretern des Parlaments und dem Ministerrat (sog. Trilog), ohne dass es bis dahin einen abschließenden Textvorschlag des Ministerrates gab. Am 15. Dezember 2015 verständigten sich Kommission, Ministerrat und Vertreter des Parlaments auf einen gemeinsamen Text[1]. Diesem Vorschlag stimmte der Ausschuss für bür-

[1] Eine Gegenüberstellung der unterschiedlichen Entwurfsfassungen mit der englischen Fassung des Trilogs ist abrufbar über die Seite des Baye-

gerliche Freiheiten, Justiz und Inneres (LIBE) des Parlaments am 17. Dezember 2015 zu. Über den erzielten Kompromiss stimmt das Parlament im Frühjahr 2016 (voraussichtlich im März oder April 2016) ab.

Die Verordnung wird daher voraussichtlich im April 2016 in Kraft treten. Sodann beginnt eine Frist von zwei Jahren, innerhalb derer die Mitgliedsländer die erforderlichen Anpassungen in nationales Recht vornehmen müssen, soweit dafür nach den Vorschriften in der Grundverordnung noch Raum ist.

Größerer Anpassungsbedarf ist für die öffentlich-rechtlichen Rundfunkanstalten zum gegenwärtigen Zeitpunkt nicht erkennbar. Art. 80 Absatz 2 der Datenschutz-Grundverordnung lässt Raum für die Fortgeltung der bestehenden deutschen Regelungen zum Medienprivileg und zu einer von staatlichen Stellen unabhängigen Datenschutzaufsicht im Rundfunk, so dass es dazu keiner Anpassungen im nationalen Recht bedarf.

Gesetz zur Vorratsdatenspeicherung

Mit Urteil vom 2. März 2010 (1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08) erklärte das Bundesverfassungsgericht die seinerzeit geltende Ausgestaltung der Vorratsdatenspeicherung für nicht verfassungsgemäß und nichtig (vgl. auch Tätigkeitsbericht 2010, Seite 7 und Anlage 2). Am 16. Oktober 2015 stimmte der Deutsche Bundestag in zweiter und dritter Lesung einem neuen Gesetz zur Vorratsdatenspeicherung zu. Danach sind Telekommunikationsunternehmen, Internetprovider und andere Zugangsanbieter verpflichtet, sogenannte Verkehrsdaten (nicht: Inhalte) zehn Wochen lang zu speichern. Standortdaten, die bei der Nutzung von Mobildiensten anfallen, sollen vier Wochen lang gespeichert werden. Außerdem wurde ein neuer Straftatbestand der Datenhehlerei eingeführt. Danach wird bestraft, wer anderen illegal beschaffte, nicht öffentliche Daten zugänglich macht.

Das Gesetz ist am 18. Dezember 2015 in Kraft getreten. Die Verpflichtung zur Speicherung von Daten wird 18 Monate nach Inkrafttreten wirksam.

Zum Gesetzgebungsvorhaben haben die ARD, der Bundesverband Deutscher Zeitungsverleger (BDZV), der Deutsche Journalistenverband (DJV), der Deutsche Presserat, der Verband Deutscher Zeitschriftenverleger (VDZ), die Vereinte Dienstleistungsgewerkschaft (dju in verdi), der Verband Privater Rundfunk und Telemedien (VPRT) und das ZDF mit Schreiben vom 7. September 2015 (**Anlage 1**) Stellung genommen. Darin kritisieren sie

---

rischen Datenschutzbeauftragten unter
https://www.lda.bayern.de/media/baylda_synopse.pdf

vor allem die Erfassung von Verkehrs- und Standortdaten von Gesprächen, die zwischen Journalistinnen und Journalisten oder zwischen Journalistinnen/Journalisten und Informantinnen/Informanten geführt werden. Sie verweisen darauf, dass damit im Einzelfall erhebliche Rückschlüsse auf das Kommunikations- und Bewegungsverhalten der Beteiligten möglich sind. Dies verstoße sowohl gegen Art. 5 Absatz 1 Satz 2 GG und Art. 10 Absatz 1 als auch gegen den besonderen Schutz journalistischer Quellen, der in dem in § 53 Abs. 2 Satz 3 StPO geregelten Zeugnisverweigerungsrecht seinen Ausdruck findet.

Die gegen das Gesetzgebungsvorhaben gerichteten verfassungsrechtlichen Bedenken finden im endgültigen Gesetzestext keinen Niederschlag. Die FDP sowie Vertreter der im Bundestag vertretenen Oppositionsparteien haben bereits angekündigt, gegen das Gesetz (erneut) vor dem Bundesverfassungsgericht klagen zu wollen.

II. Rechtsprechung

- Entscheidung des Gerichtshofs der Europäischen Union vom 6. Oktober 2015 zur Ungültigkeit der Safe Harbor-Entscheidung der Kommission aus dem Jahr 2000.
- Urteil des Bundesarbeitsgerichts vom 19. Februar 2015 zur Unzulässigkeit einer Observation durch einen Detektiv mit heimlich hergestellten Videoaufnahmen.

Einzelheiten zu diesen Entscheidungen sind in der **Anlage 2** dargestellt.

E. Tätigkeit des Datenschutzbeauftragten im NDR im Berichtszeitraum

I. Arbeitsstrukturen und -schwerpunkte

Im Berichtszeitraum standen datenschutzrechtliche Fragen vor allem aus den Bereichen

- **Redaktionsdatenschutz/Redaktionsgeheimnis,**
- **Evaluierung der Datenschutzbestimmungen im Rundfunkbeitragsstaatsvertrag,**
- **Teilnehmerdatenverwaltung,**
- **Personaldatenverwaltung,**
- **Organisations- und Strukturprojekte** zur Verbesserung konzeptioneller und arbeitstechnischer Abläufe.

im Vordergrund.

Soweit der NDR personenbezogene Daten **ausschließlich zu eigenen journalistisch-redaktionellen Zwecken** verarbeitet, gelten gemäß § 42 Abs. 1 NDR Staatsvertrag nur die Vorschriften in §§ 7 und 8 des Hamburgischen Datenschutzgesetzes über die Wahrung des Datengeheimnisses sowie über technische und organisatorische Maßnahmen zum Schutz insbesondere gegenüber Zugriffen Unbefugter bei der Bearbeitung, bei der Aufbewahrung, beim Transport und bei der Vernichtung dieser Daten (sogenanntes „Medienprivileg"). In diesem Zusammenhang beschränkte sich die Tätigkeit des Datenschutzbeauftragten auf die Beantwortung von Einzelanfragen.

Bei der Teilnehmerdatenverwaltung sind ständige Ansprechpartner zum einen die Abteilung Beitragsservice des NDR, zum anderen **der ARD ZDF und Deutschlandradio Beitragsservice in Köln.** Während mit der Abteilung Beitragsservice für gewöhnlich Einzelfälle zur Diskussion stehen, konzentriert sich die Zusammenarbeit mit dem Zentralen Beitragsservice auf die Sicherstellung der datenschutzrechtlichen Unbedenklichkeit des dort abzuwickelnden Massenverfahrens.

II. Einzelthemen

Evaluierung der Datenschutzbestimmungen im Rundfunk-Beitragsstaatsvertrag (RBStV)

Die Bundesländer hatten im Zusammenhang mit dem Inkrafttreten des Beitragsstaatsvertrages am 1. Januar 2013 beschlossen, die darin enthaltenen Datenschutzbestimmungen einer Überprüfung zu unterziehen. Dazu fand am 21. Oktober 2014 eine erste Besprechung mit Vertretern der Länder, den Landesbeauftragten für den Datenschutz (und Informationsfreiheit), Vertretern der Landesrundfunkanstalten und des Zentralen Beitragsservice für ARD, ZDF und Deutschlandradio und den Rundfunkbeauftragten für den Datenschutz statt (vgl. Tätigkeitsbericht 2014, Seite 5). Für den Arbeitskreis der Rundfunkbeauftragten für den Datenschutz (AK DSB) nahm der NDR Datenschutzbeauftragte mit Schreiben vom 30. Januar 2015 **(Anlage 3)** schriftlich Stellung. Dabei widmete er besondere Aufmerksamkeit der Frage, ob ein erneuter vollständiger Meldedatenabgleich datenschutzrechtlich zulässig ist oder nicht.

Diese schriftlichen Ausführungen vertiefte er noch einmal in der Anhörung der Rundfunkreferenten zum Entwurf eines novellierten Rundfunkbeitragsstaatsvertrages am 5. August 2015 in Berlin. Der Bewertung der Rundfunkbeauftragten für den Datenschutz folgend war darin ein erneuter vollständiger Meldedatenabgleich vorgesehen. Diesem gesetzgeberischen Vorhaben widersprach der Berliner Beauftragte für Datenschutz und Informationsfreiheit als Vertreter der Landesbeauftragten für

Datenschutz (und Informationsfreiheit) mit der Begründung, dass das gesetzgeberische Ziel, mit der Umstellung des Systems die Gefahr eines Rückgangs von Beitragskonten auszuschließen, mit der Durchführung des einmaligen Meldedatenabgleichs erfüllt sei. Einer Verschlechterung des Datenbestandes könne durch die regelmäßigen anlassbezogenen Datenübermittlungen entgegengewirkt werden, so dass eine Wiederholung des vollständigen Meldedatenabgleichs nicht erforderlich sei.

Der von den Ministerpräsidenten am 8./9. Oktober 2015 unterzeichnete 19. Rundfunkänderungsstaatsvertrag enthält eine Regelung zur Wiederholung des vollständigen Meldedatenabgleichs.

Personalisierung von Mediatheken

Am 22. Juni 2015 stellte die Leiterin der Redaktion von ard.de, Frau Heide Schmidt, beim SWR in Mainz erste Überlegungen zur Personalisierung von Mediatheken vor. In einer ersten datenschutzrechtlichen Bewertung haben die Rundfunkbeauftragten für den Datenschutz darauf hingewiesen, dass für die dabei vorgesehene Verarbeitung personenbezogener Daten ausdrücklich die Zustimmung der Nutzerinnen und Nutzer der Mediatheken eingeholt und nachgehalten werden muss. Außerdem müssen die Nutzerinnen und Nutzer die Möglichkeit erhalten, ihre Zustimmung jederzeit und ohne Angabe von Gründen zu widerrufen.

Die Rundfunkbeauftragten für den Datenschutz haben ferner darauf hingewiesen, dass die Einholung der Zustimmung von Kindern und Jugendlichen besondere Anforderungen stellt, da insoweit auf Altersgrenzen und die Einsichtsfähigkeit der Betroffenen Rücksicht genommen werden muss.

Die Redaktion hat es übernommen, Einzelheiten in einer Datenschutz-Charta zu regeln und mit dem Arbeitskreis der Rundfunkbeauftragten für den Datenschutz abzustimmen.

III. Befassung mit Projekten und Vorhaben zur Verarbeitung personenbezogener Daten im NDR

Im Berichtszeitraum hat der Datenschutzbeauftragte insgesamt 23 Projekte vorab geprüft, in deren Rahmen die Speicherung und/oder Verarbeitung personenbezogener Daten in Betracht kam. Mit dieser sogenannten Vorabkontrolle (vgl. § 8 Absatz 4 HmbDSG und § 4d Absatz 5 Satz 1 BDSG) nimmt er eine der wesentlichen Aufgaben für Datenschutzbeauftragte wahr.

Eine chronologische Aufstellung der Projekte, zu denen ein datenschutzrechtliches Votum abgegeben wurde, ist als **Anlage 4** diesem Bericht beigefügt.

Die Anzahl der im Rahmen einer Vorabprüfung beurteilten Projekte war geringfügig höher als die Anzahl der im Vorjahr geprüften 21 Projekte, bewegte sich aber im durchschnittlichen Mittel der letzten Jahre.

IV. Standardisierte Anträge auf Zustimmung durch den NDR Datenschutzbeauftragten

Im Jahr 2015 ist die Zahl der DV-Einzelbedarfsanträge gegenüber den im Jahr 2014 insgesamt 953 geprüften Anträgen deutlich zurückgegangen und erreicht in etwa wieder die Größenordnung der 2013 geprüften Anträge (770). Die DV-Einzelbedarfsanforderungen werden summarisch auf eventuelle datenschutzrechtliche Relevanz hin überprüft. Darin enthalten ist regelmäßig eine größere Anzahl von Beschaffungsmaßnahmen, bei denen erkennbar datenschutzrechtliche Fragen nicht berührt sind. Deswegen wurde unter der Federführung des Bereiches Informations-, Medien- und Verbreitungstechnik im Jahr 2014 der Workflow einer kritischen Prüfung unterzogen, um auch eine Entlastung des Datenschutzbeauftragten von datenschutzrechtlich nicht relevanten Vorgängen zu erreichen. Diese Untersuchung wurde im Juli 2014 abgeschlossen. Sie wurde durch ein Feinkonzept für die Umsetzung ergänzt. Der geänderte Workflow wird 2016 umgesetzt.

V. Schulungen für Mitarbeiter des NDR

Der Datenschutzbeauftragte hat auch im Jahre 2015 Schulungen für Mitarbeiterinnen und Mitarbeiter des NDR abgehalten:

13.01.2015	Mitarbeiterinnen und Mitarbeiter des Bereichs Service Informationssysteme (SIS) in der Produktionsdirektion
21.01.2015	Mitarbeiterinnen und Mitarbeiter in der Programmdirektion Fernsehen, Programmbereich Ausland und Aktuelles
13.04.2015	Mitarbeiterinnen und Mitarbeiter des Bereichs Service Informationssysteme (SIS) in der Produktionsdirektion

15.04.2015	Mitarbeiterinnen und Mitarbeiter der Hauptabteilung Personal
28.04.2015	Mitarbeiterinnen und Mitarbeiter in der Programmdirektion Fernsehen, Programmbereich Wirtschaft & Ratgeber
11.05.2015	Mitarbeiterinnen und Mitarbeiter des Bereichs Service Informationssysteme (SIS) in der Produktionsdirektion
13.05.2015	Mitarbeiterinnen und Mitarbeiter des Bereichs Projekte und Technologie für IT und Medien (PTIM) in der Produktionsdirektion
04.08.2015	Auszubildende Technik
15.09.2015	Programmvolontärinnen und Programmvolontäre
22.09.2015	Mitarbeiterinnen und Mitarbeiter des Gebäudemanagements in der Verwaltungsdirektion im Zusammenhang mit der Einführung eines neuen Zutrittskontrollsystems
18.11.2015	Auszubildende, Mitarbeiterinnen und Mitarbeiter in der Verwaltung und Personalräte im Landesfunkhaus Mecklenburg-Vorpommern

Im Rahmen dieser Schulungen sind insgesamt 211 Mitarbeiterinnen und Mitarbeiter des NDR mit Fragen des Datenschutzes erstmals oder erneut vertraut gemacht worden. Die Anzahl geschulter Mitarbeiterinnen und Mitarbeiter lag erheblich über dem langjährigen Durchschnitt von ca. 100 geschulten Mitarbeitern.

Ähnlich wie im Berichtszeiträumen 2014 wurden auch im Jahr 2015 zahlreiche Mitarbeiterinnen und Mitarbeitern in der Programmdirektion Fernsehen geschult, wobei die durchgeführten Schulungen auch den dort beschäftigten freien Mitarbeiterin-

nen und Mitarbeitern angeboten und von diesen wahrgenommen wurden.

VI. Eingaben beim NDR Datenschutzbeauftragten

Nach § 40 Absatz 8 NDR-Staatsvertrag kann sich jede Bürgerin und jeder Bürger an den Datenschutzbeauftragten wenden, wenn er oder sie der Ansicht ist, bei der Verarbeitung personenbezogener Daten durch den NDR oder durch Dritte, die in seinem Auftrag tätig wurden, in ihren oder seinen schutzwürdigen Interessen verletzt worden zu sein. Von diesem Recht haben im Berichtszeitraum 25 Bürgerinnen und Bürger Gebrauch gemacht. Dies lag deutlich unter der Anzahl von Eingaben, die im Jahr 2014 (36 Eingaben) an den Datenschutzbeauftragten gerichtet wurden. Die Anzahl der Eingaben bewegt sich allerdings innerhalb der langjährigen Schwankungsbreite zwischen 20 und 50 Eingaben.

Als **Anlage 5** wird eine Zusammenstellung des jeweiligen Gegenstandes der Eingaben vorgelegt. Die Aufstellung macht deutlich, dass auch im Berichtszeitraum der ganz überwiegende Anteil der Eingaben allgemeine Fragen nach der Zulässigkeit von Vorgehens- und/oder Verfahrensweisen beim Rundfunkbeitragseinzug betrifft und somit keine Beschwerden im eigentlichen Sinn darstellen.

Anlass zu förmlichen Beanstandungen gab es im Berichtszeitraum nicht.

VII. Datenschutzrechtlich relevante Vorfälle

Im Berichtszeitraum gab es keine datenschutzrechtlich relevanten Vorgänge. Die Störung des Internetauftritts und des internen Netzwerkes von „TV 5 Monde“ in Frankreich wurde vom IT-Sicherheitsbeauftragten zum Anlass genommen, in Abstimmung mit dem Datenschutzbeauftragten die Sicherheit des NDR-Netzes und des Internetauftritts des NDR und seiner Programme einer kritischen Überprüfung zu unterziehen. Dabei wurden keine erkennbaren Schwachstellen gefunden.

F. Externe Prüfungen

I. Informations-Verarbeitungs-Zentrum (IVZ)

Beim Rundfunk Berlin-Brandenburg (rbb) wird als Gemeinschaftseinrichtung des Deutschlandradios, des MDR, des NDR, von RB, des RBB, des SR und des WDR das Informations-Verarbeitungs-Zentrum (IVZ) betrieben. Dort werden für die beteiligten Anstalten zentral Aufgaben der elektronischen Datenverarbeitung abgewickelt.

Am 1. Dezember 2015 fand beim IVZ das jährliche Treffen der Datenschutzbeauftragten der beteiligten Anstalten und des IVZ statt, um datenschutzrechtliche Details zu erörtern. Dieses Treffen hat die Stellvertretende Datenschutzbeauftragte wahrgenommen. Dabei haben sich keine Anhaltspunkte ergeben, die ein Tätigwerden des Datenschutzbeauftragten erfordert hätten.

II. Beihilfe- und Bezüge-Zentrum GmbH (bbz)

Bei vorangegangenen Prüfungen waren nicht unerhebliche datenschutzrechtliche Probleme festgestellt worden (vgl. Tätigkeitsbericht 2014, Seite 9 f.). Am 24. Juni 2015 fand eine erneute Datenschutzprüfung statt, an der für den NDR die Stellvertretende Datenschutzbeauftragte teilnahm.

Dabei wurde festgestellt, dass das bereits seit längerem geforderte IT-Sicherheitskonzept zum Ende des Jahres 2013 erstellt und zur Diskussion gestellt worden war. Kritisierte Einzelpunkte wurden, beratend unterstützt vom IT-Sicherheitsbeauftragten des ZDF, verbessert. Eine Risikoanalyse zur abschließenden Ermittlung des Schutzbedarfs wurde, einer Forderung aus den Prüfungen folgend, erstellt.

Der in den letzten Prüfungen geübten Kritik an der Anbindung von PC, an denen Beihilfevorgänge bearbeitet werden, an das Internet wird im vorgelegten Sicherheitskonzept durch erhöhte Sicherheitsmaßnahmen und Einschränkungen Rechnung getragen. Eine den Internetzugang beschränkende White-List für die Beihilfesachbearbeitung ist bereits umgesetzt. Nach Aussage des betrieblichen Datenschutzbeauftragten haben lediglich fünf Mitarbeiterinnen und Mitarbeiter im Bereich Sondersachbearbeitung uneingeschränkten Internetzugriff.

Zusätzlich zum externen betrieblichen Datenschutzbeauftragten und einem Beauftragten für Arbeitssicherheit soll ein Beauftragter für IT-Sicherheit bestellt werden.

III. Baden-Badener Pensionskasse

Das Rechenzentrum des IVZ in Köln hat inzwischen die Erbringung der IT-Dienstleistungen für die Baden-Badener Pensionskasse (bbp) übernommen. Anlässlich eines Besuches im Rechenzentrum am 20. Oktober 2015 haben sich Rundfunk-Datenschutzbeauftragte, darunter auch der NDR Datenschutzbeauftragte, Einzelheiten des Betriebskonzeptes erläutern lassen. Ergänzend wurde den Datenschutzbeauftragten das Ergebnis der Prüfung der Informationssicherheit im August 2015 zur Verfügung gestellt.

Es haben sich keine Anhaltspunkte ergeben, die ein Tätigwerden der Datenschutzbeauftragten erfordert hätten.

G. Zusammenarbeit mit anderen Datenschutzbeauftragten

I. Arbeitsgruppe nach Art. 29 der EG-Datenschutzrichtlinie

Der NDR hat, wie in den Vorjahren, auch im Jahr 2015 den AK DSB in der **Datenschutzarbeitsgruppe nach Art. 29 EG-Datenschutzrichtlinie** vertreten. Der AK DSB wird durch den NDR regelmäßig über die Tätigkeiten und Initiativen der Art. 29-Arbeitsgruppe informiert.

II. Arbeitskreis der Rundfunkbeauftragten für den Datenschutz (AK DSB)

Der Arbeitskreis der Rundfunkbeauftragten für den Datenschutz ist im Berichtszeitraum insgesamt zweimal, und zwar am 12./13. März 2015 im Landestudio des Südwestrundfunks in Karlsruhe und am 24./25. September 2015 bei Arte in Straßburg, zusammengekommen. Die thematischen Schwerpunkte, mit denen sich der AK DSB in seinen beiden Sitzungen befasst hat, sind in der **Anlage 6** zu diesem Bericht zusammengestellt.

Im Berichtszeitraum war der Datenschutzbeauftragte des ZDF Vorsitzender des AK DSB und der NDR-Datenschutzbeauftragte sein Stellvertreter.

III. Arbeitskreis Medien der Landesdatenschutzbeauftragten

Die Rundfunkbeauftragten für den Datenschutz pflegen einen regelmäßigen Informationsaustausch mit dem Arbeitskreis Medien der Beauftragten für den Datenschutz des Bundes und der Länder. Dazu nimmt der Vorsitzende des Arbeitskreises Medien zeitweise an den Sitzungen des AK DSB und umgekehrt eine Vertreterin oder ein Vertreter des AK DSB an den Sitzungen des AK Medien teil. Im Berichtszeitraum hat die Datenschutzbeauftragte des Rundfunks Berlin-Brandenburg den AK DSB in den Sitzungen des AK Medien vertreten.

IV. Das virtuelle Datenschutzbüro

Der NDR Datenschutzbeauftragte beteiligt sich als sogenannter Projektpartner an dem vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) technisch organisierten "Virtuellen Datenschutzbüro" (VirDSB). Das VirDSB ist ein ge-

meinsamer Service vorrangig der deutschen Datenschutzinstitutionen, dargestellt als Datenschutz-Portal (http://www.datenschutz.de). Angeboten werden hier Informationen vom datenschutzrechtlichen Grundwissen bis hin zu Informationen für Experten. Die Online-Angebote des NDR Datenschutzbeauftragten und des VirDSB verlinken auf das jeweils andere Angebot. Am Projektpartnertreffen am 24. Februar 2015 in Hannover nahm der NDR Datenschutzbeauftragte teil. Am Projektpartnertreffen am 27. Oktober 2015 haben leider weder der Datenschutzbeauftragte noch die Stellvertretende Datenschutzbeauftragte teilgenommen.

H. Zielsetzungen und Perspektiven

Das Jahr 2016 wird vor allem durch die Umsetzung der europäischen Datenschutz-Grundverordnung und damit zusammenhängender Fragen geprägt sein. Wesentliche Auswirkungen auf die Arbeit der Rundfunk-Datenschutzbeauftragten sind dabei nach der finalen Fassung des Verordnungstextes allerdings nicht zu erwarten.

Hamburg, den 16. Februar 2015

ARD • BDZV • DJV • Deutscher Presserat

VDZ • ver.di • VPRT • ZDF

---

7. September 2015

Gemeinsame Stellungnahme

zum Entwurf eines Gesetzes der Bundesregierung und der Fraktionen CDU/CSU und SPD zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (BT-Drs. 18/5171; BT-Drs. 18/5088)

von

Arbeitsgemeinschaft der öffentlich-rechtlichen Rundfunkanstalten (ARD)

Bundesverband Deutscher Zeitungsverleger (BDZV)

Deutscher Journalisten-Verband (DJV)

Deutscher Presserat

Verband Deutscher Zeitschriftenverleger (VDZ)

Vereinte Dienstleistungsgewerkschaft (dju in ver.di)

Verband Privater Rundfunk und Telemedien (VPRT)

Zweites Deutsches Fernsehen (ZDF)

A.

1. Mit der Rechtsprechung des EuGH zum Verhältnis von Berufsgeheimnis und Vorratsdatenspeicherung sind die vorgeschlagenen Regelungen, insbesondere § 100g Abs. 4 StPO, nicht in Einklang zu bringen.

2. Beim Umgang mit personenbezogenen Daten sind - vor allem im Hinblick auf den Erhalt der journalistischen Berichterstattungsfreiheit - enge rechtliche Grenzen zu wahren. Sowohl das Bundesverfassungsgericht als auch der Europäische Gerichtshof haben diese Grenzen in Entscheidungen konkretisiert. Auch der vorliegende, vom Bundeskabinett am 27. Mai 2015 verabschiedete Gesetzentwurf zur Einführung der Speicherung, Erhebung und Verwendung

von Verkehrsdaten auf Vorrat zu Strafverfolgungszwecken und Zwecken der Gefahrenabwehr (Vorratsdatenspeicherung), muss den Anforderungen des Europäischen Gerichtshofs in seinem Urteil vom 8. April 2014 zur Richtlinie 2006/24/EG und denen des Bundesverfassungsgerichts in seinem Urteil vom 2. März 2010 (BVerfGE 125,260) genügen. Das ist nicht der Fall.

3. Die im Entwurf vorgesehene anlasslose Speicherung von u. a. Verkehrsdaten ist weder verfassungsrechtlich noch europarechtlich zu rechtfertigen, da danach deren Erforderlichkeit zu Zwecken der Gefahrenabwehr oder der Strafverfolgung nicht stets zweifelsfrei nachgewiesen werden muss. Die anlasslose Speicherung, Erhebung und sonstige Verwendung solcher Daten auf Vorrat ist mit dem national und auf europäischer Ebene garantierten Recht auf informationelle Selbstbestimmung und den hieraus erwachsenden datenschutzrechtlichen Grundsätzen der Erforderlichkeit und der Datensparsamkeit nicht zu vereinbaren und deswegen unzulässig und stellt in der vorgesehen Form auch einen massiven Eingriff in die Bürgerrechte dar.

4. Die Speicherung, Erhebung und sonstige Verwendung von Telekommunikationsdaten auf Vorrat für Zwecke der Gefahrenabwehr bzw. der Strafverfolgung greift überdies in besonderem Maße in die Vertrauensverhältnisse von Berufsgeheimnisträgern, hier: der Journalistinnen und Journalisten, ein. Bereits die Speicherung von Telekommunikationsdaten bei Verpflichteten nach dem TKG (§ 113a TKG) ermöglicht, diese vertrauliche Kommunikation nachzuvollziehen. Vorgesehen ist zudem die Erhebung von Standortdaten zum Zwecke der Anfertigung von Bewegungsprofilen. Jede Maßnahme für sich, aber auch deren Verknüpfung, ist geeignet, das Vertrauen in den Informantenschutz nachhaltig zu untergraben bzw. gar nicht erst aufkommen zu lassen. Das gefährdet die journalistische Berichterstattungsfreiheit in nicht hinnehmbarem Maße. Das Vorhaben der Bundesregierung bedarf unter diesem Gesichtspunkt einer besonders strengen Überprüfung. Erst recht ist die Erhebung der Daten für den späteren Zugriff durch Strafverfolgungsbehörden bzw. zur Gefahrenabwehr daraufhin zu untersuchen, ob der Informantenschutz noch effektiv gewährleistet wird. Das ist nach dem vorliegenden Entwurf nicht der Fall.

5. Unter den notwendigen Verfahrensgarantien einer Rechtsordnung ist nach der Rechtsprechung des Europäischen Menschenrechtsgerichtshofs (EGMR) zuerst und vor allem die Garantie notwendig, dass ein Gericht und nicht etwa die Staatsanwaltschaft über Ermittlungsmaßnahmen entscheidet, bevor die Ermittlungsbehörden sich Zugang zu dem Informantenschutz oder dem Redaktionsgeheimnis unterliegenden journalistischen Quellen verschaffen.

6. Art. 5 (§ 202d StGB-E) des geplanten Gesetzes ist trotz der vorgesehenen Regelung in § 202d Abs. 3 Nr. 2 StGB-E als eine Schwächung des Informantenschutzes und des Redaktionsgeheimnisses und damit als eine erhebliche Beeinträchtigung der Presse- und Rundfunkfreiheit anzusehen, insbesondere, weil die Ausnahmeregelung in § 202d Abs. 3 StGB-E lediglich journalistische Tätigkeiten in Vorbereitung einer konkreten Veröffentlichung umfasst.

B.

I. Vorhaben der Bundesregierung und der Fraktionen von CDU/CSU und SPD

Mit dem vorgelegten Gesetzentwurf beabsichtigen die Bundesregierung und die Fraktionen von CDU/CSU und SPD, eine Regelung zur zeitlich befristeten Speicherung von Verkehrsdaten und Standortdaten zur Gefahrenabwehr und zur Strafverfolgung zu schaffen. Die damit verbundenen Eingriffe in das Recht auf informelle Selbstbestimmung, die freie Entfaltung der Persönlichkeit, die Kommunikationsgrundrechte und das Fernmeldegeheimnis (Art. 2, 5, 10 GG; Art. 7, 8 und 11 der Grundrechtecharta der Europäischen Union) sollen sich dabei nach Ansicht der Bundesregierung noch in zulässigem Rahmen bewegen.

1) Im Einzelnen sieht der Gesetzentwurf vor:

a) die Speicherung von Verkehrsdaten (§ 96 Abs. 1 TKG) bei Verdacht einer Straftat mittels Telekommunikation bzw. einer im Einzelfall erheblich bedeutenden Straftat,

b) die Speicherung von Verkehrsdaten nach § 113b TKG bei auch im Einzelfall besonders schwerwiegenden, im Einzelnen aufgeführten Straftaten,

c) die Speicherung aller in einer Funkzelle angefallenen Verkehrsdaten bei Verdacht einer Straftat auch im Einzelfall von erheblicher Bedeutung bzw. der nach § 113b TKG angefallenen Verkehrsdaten unter der Voraussetzung des Verdachts einer besonders schweren Straftat,

d) die Erhebung (bzw. den Abruf) der Daten zu den genannten Zwecken durch die Strafverfolgungsbehörden und die Polizeibehörden sowie durch Telekommunikationsunternehmen für eine Bestandsdatenauskunft nach § 113 Abs. 1 Satz 3 TKG,

e) einen Richtervorbehalt ohne Eilkompetenz der Staatsanwaltschaften, soweit nicht Verkehrsdaten nach § 96 TKG oder eine Funkzellenabfrage außerhalb des Anwendungsbereichs des § 113b TKG i.V.m. § 100g Abs. 2 StPO betroffen ist,

f) eine qualifizierte Begründungspflicht für Maßnahmen zur Datenspeicherung hinsichtlich der Erforderlichkeit und Angemessenheit einer Maßnahme,

g) eine Regelung zur Weiterabe der erhobenen Daten an andere Stellen nur unter Einhaltung der o. a. Verwendungszwecke,

h) eine Benachrichtigungs- und Anhörungspflicht vor der Entscheidung über die Zulässigkeit einer Anordnung des Abrufs der erhobenen Daten, es sei denn, der Zweck der Anordnung würde gefährdet,

i) eine Speicherpflicht, die sich auf die Pflicht zur Speicherung der Daten im Inland bezieht,

j) Regelungen zur Datensicherheit,

k) Löschungsregelungen entsprechend § 101 Abs. 8 StPO bzw. eine Vorschrift zur irreversiblen Löschung der gespeicherten Daten nach Ablauf der Speicherfristen (10 Wochen bzw. 4 Wochen bei Standortdaten),

l) die Speicherungspflicht von Verkehrsdaten auch von Berufsgeheimnisträgern, während die Erhebung dieser Daten durch die genannten Behörden unzulässig sein soll, soweit sie sich gegen eine zeugnisverweigerungsberechtigte Person richtet und die Erhebung voraussichtliche Erkenntnisse erbringen würde, über die diese das Zeugnis verweigern dürfte.

2) Für die Speicherung in Frage kommende Verkehrsdaten nach § 96 TKG sind:

a) Nummern oder Kennungen beteiligter Anschlüsse oder Endeinrichtungen, personenbezogene Berechtigungskennungen, Nummern von Kundenkarten sowie Standortdaten mobiler Anschlüsse,

b) der Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und Übermittelte Datenmengen,

c) der Name des in Anspruch genommenen Telekommunikationsdienstes

d) sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten.

3) Verkehrsdaten nach § 113b TKG sind:

a) Rufnummern oder Kennungen der beteiligten Anschlüsse,

b) Datum und Uhrzeit von Beginn und Ende der Verbindung (inkl. Zeitzone),

c) Angaben zur den genutzten Diensten,

d) im Falle mobiler Telefondienste die internationale Kennung der beteiligten Anschlüsse bzw. Geräte sowie das Datum und die Uhrzeit der ersten Aktivierung des Dienstes (inkl. Zeitzone), wenn Dienste im Voraus gezahlt wurden,

e) im Fall von Internet-Telefondiensten die Internetprotokolladressen der beteiligten Anschlüsse sowie die zugewiesenen Benutzerkennungen,

f) bei der Inanspruchnahme öffentlich zugänglicher Internetzugangsdienste die dem Teilnehmer zugewiesene Internetprotokolladresse, die Kennung des Anschlusses, über die die Internetnutzung erfolgt sowie die zugewiesene Benutzerkennung und Datum und Uhrzeit von Beginn und Ende der Internetnutzung (inkl. der Zeitzone). Bei Inanspruchnahme von Funkzellen sind die zu Beginn der Verbindung genutzten Zellen zu speichern sowie die geografische Lage und die Hauptstrahlrichtung der die jeweilige Funkzelle versorgenden Funkantennen.

4) Nicht gespeichert werden dürfen der Inhalt der Kommunikation, Daten über aufgerufene Internetseiten und Daten von Diensten der elektronischen Post (nach § 113b TKG) sowie Daten von Verbindungen zum Zweck der Beratung in seelischen oder sozialen Notlagen, soweit Personen oder deren Mitarbeiter insoweit besonderen Verschwiegenheitsverpflichtungen unterliegen.

II. Allgemeine Bewertung des Gesetzentwurfs

1) Anwendung europäischen Rechts

Der Europäische Gerichtshof (EuGH) hat mit Urteil vom 8. April 2014[1] die Richtlinie zur Vorratsdatenspeicherung in der EU (2006/24/EG) für ungültig erklärt, weil die Richtlinie gegen die Grundrechtecharta der EU, insbesondere gegen Art. 7 und 8 verstieß. Die nach der Richtlinie für eine Dauer von mindestens sechs Monaten zu speichernden Daten entsprachen den Daten, die nunmehr nach der Absicht der Bundesregierung für die Dauer von zehn bzw. vier Wochen zu speichern, zu erheben und unter den vorgesehenen Voraussetzungen zu nutzen sind.

Nachdem die Richtlinie 2006/24/EG als Rechtsgrundlage für die Vorratsdatenspeicherung aufgrund des Urteils des EuGH weggefallen ist, bleibt als europarechtliche Grundlage noch Art. 15

[1] vgl. EuGH, Vorabentscheidungsersuchen nach Art. 267 AEUV, eingereicht vom High Court (Irland) und vom Verfassungsgerichtshof (Österreich), Az.: C-293/12 und C-594/12, ZUM-RD 2014,333

Abs. 1 der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation), die die Datenspeicherung zur Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten grundsätzlich zulässt, da durch Verweis auf Art. 6 Abs. 1 und Abs. 2 des Vertrages über die Europäische Union die Mitgliedsstaaten verpflichtet sind, die Charta der Grundrechte der EU zu beachten. Die Gesetzgebung zur Vorratsdatenspeicherung unterliegt damit der Bindung an die Charta[2].

2) Urteil des EuGH

Der EuGH hat sich bei der Ungültigkeitserklärung der Richtlinie 2006/24/EG vor allem auf die Achtung des Privat- und Familienlebens (Artikel 7 der Grundrechtecharta) und den Schutz personenbezogener Daten (Artikel 8), daneben aber auch auf die Freiheit der Meinungsäußerung und Informationsfreiheit (Artikel 11) gestützt.

Zwar ist nach dem Urteil des EuGH die Speicherung von Verkehrsdaten auf Vorrat zur Bekämpfung von Kriminalität nicht gänzlich ausgeschlossen, weil angesichts der wachsenden Bedeutung elektronischer Kommunikationsmittel die gespeicherten Daten den für die Strafverfolgung zuständigen nationalen Behörden zusätzliche Möglichkeiten zur Aufklärung schwerer Straftaten bieten und daher ein nützliches, geeignetes Mittel für strafrechtliche Ermittlungen darstellen[3]. Die Bekämpfung schwerer Kriminalität, z. B. des internationalen Terrorismus zur Gewährleistung der öffentlichen Sicherheit sei eine dem Gemeinwohl dienende Zielsetzung[4].

Der Wesensgehalt der Achtung der Privatsphäre, des Schutzes personenbezogener Daten und der Meinungsfreiheit wird durch eine Vorratsdatenspeicherung nach Ansicht des EuGH nicht zwingend angetastet, solange sie den Inhalt der elektronischen Kommunikation nicht zur Kenntnis gibt, die Grundsätze des Datenschutzes und der Datensicherheit eingehalten werden sowie die Inhalte von Nachrichten und der mit Hilfe eines elektronischen Kommunikationsnetzes abgerufenen Informationen nicht offen gelegt werden[5].

Dies sei jedoch bei der Vorratsdatenspeicherung, wie sie der EuGH zu beurteilen hatte, nicht der Fall gewesen. Diese beinhalte einen Eingriff in die genannten Grundrechte von großem

---

2 so auch Gesetzentwurf der Bundesregierung, S. 24

3 vgl. Urteil des EuGH, aaO, Rdnr. 49

4 vgl. Urteil des EuGH, aaO, Rdnr. 42 ff., 44

5 vgl. Urteil des EuGH, aaO, Rdnr. 28, 39 und 40

Ausmaß, der als besonders schwerwiegend anzusehen sei[6]. Dieser Eingriff müsse, um rechtmäßig zu sein, nicht nur geeignet sein, die verfolgte Zielsetzung zu erreichen. Er müsse auch erforderlich und verhältnismäßig sein, dürfe also die Grenzen dessen nicht überschreiten, was zur Erreichung des Ziels geeignet und erforderlich sei[7]. Der Gestaltungspielraum des Unionsgesetzgebers, aber auch des nationalen Gesetzgebers, soweit er wie hier an das Unionsrecht gebunden ist, sei, soweit es sich um Grundrechtseingriffe handelt, durch Gesichtspunkte wie den des betroffenen Bereichs, des Wesens des durch die Charta gewährleisteten Rechts, der Art und Schwere des Eingriffs sowie des Zwecks des Eingriffs begrenzt[8].

Die Bekämpfung schwerer Kriminalität, insbesondere der organisierten Kriminalität und des Terrorismus, ist zwar nach der Rechtsprechung des EuGH von größter Bedeutung für die Gewährleistung der öffentlichen Sicherheit und deren Effektivität kann in hohem Maß von der Nutzung moderner Ermittlungstechniken abhängen. Der EuGH unterstreicht jedoch, dass diese dem Gemeinwohl dienende Zielsetzung die Erforderlichkeit einer Speicherungsmaßnahme für die Kriminalitätsbekämpfung für sich genommen aber nicht rechtfertigen kann, soweit die Speicherung auf Vorrat, also anlasslos und ohne jede Differenzierung vorgenommen wird[9].

Nach der Rechtsprechung des EuGH muss eine Regelung zur Vorratsdatenspeicherung klare und präzise Regeln für die Tragweite und die Anwendung der fraglichen Maßnahme vorsehen sowie Mindestanforderungen, die einen wirksamen Schutz der personenbezogenen Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen[10]. Dieses Erfordernis gilt insbesondere dann, wenn personenbezogene Daten automatisch verarbeitet werden und eine erhebliche Gefahr des unberechtigten Zugangs zu diesen Daten besteht[11].

Zudem verlangt der Schutz des Grundrechts auf Achtung des Privatlebens nach der Rechtsprechung des EuGH, dass sich Ausnahmen vom Schutz personenbezogener Daten und die Einschränkungen dieses Schutzes auf das absolut Notwendige beschränken müssen[12]. Der Eingriff in das Grundrecht auf Privatsphäre und andere Grundrechte könne nicht als absolut notwendig bezeichnet werden, wenn alle Verkehrsdaten des Telefonfestnetzes, des Mobilfunks, des Internetzugangs und der Internettelefonie gespeichert werden, ohne einen Zusammenhang zwischen

---

6 vgl. Urteil des EuGH, aaO, Rdnr. 37
7 vgl. Urteil des EuGH, aaO, Rdnr. 46
8 vgl. Urteil des EuGH, aaO, Rdnr. 47
9 vgl. Urteil des EuGH, aaO, Rdnr. 51
10 vgl. Urteil des EuGH, aaO, Rdnr. 54
11 vgl. Urteil des EuGH, aaO, Rdnr. 55
12 vgl. Urteil des EuGH, aaO, Rdnr. 52

den auf Vorrat gespeicherten Daten und einer Bedrohung der öffentlichen Sicherheit zu verlangen[13] und ohne Ausnahmen vorzunehmen, die für Personen gelten, deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen[14].

3) Urteil des Bundesverfassungsgerichts

Das Bundesverfassungsgericht kommt in seinem Urteil vom 2. März 2010[15] zu dem Schluss, dass eine anlasslose Speicherung von Verkehrsdaten für qualifizierte Verwendungen im Rahmen der Strafverfolgung, der Gefahrenabwehr und der Aufgaben der Nachrichtendienste nicht per se und schlechthin mit dem Grundgesetz, insbesondere dem durch Art. 10 GG gewährleisteten Brief- und Fernmeldegeheimnis, unvereinbar ist[16]. Das Bundesverfassungsgericht lässt sich dabei, anders als der EuGH, von der Überlegung leiten, dass durch die anlasslose Vorratsdatenspeicherung „Aufklärungsmöglichkeiten geschaffen (werden), die sonst nicht bestünden und angesichts der zunehmenden Bedeutung der Telekommunikation auch für die Vorbereitung und Begehung von Straftaten in vielen Fällen erfolgversprechend sind."[17] Diese Speicherung von Verkehrsdaten zu Zwecken der Kriminalitätsbekämpfung sei nicht nur geeignet, sondern auch erforderlich[18] und unter genau bestimmten Voraussetzungen[19] auch verhältnismäßig[20].

Das Bundesverfassungsgericht hat allerdings empirische Befunde zur Vorratsdatenspeicherung nicht berücksichtigen können, da diese erst nach der Entscheidung veröffentlicht wurden. Es hat jedoch darauf hingewiesen, dass eine Gesetzgebung zur Vorratsdatenspeicherung zwar nicht berücksichtigen müsse, dass das Regelungsziel in jedem Einzelfall tatsächlich erreicht wird. Wohl aber werde von der Gesetzgebung verlangt, dass durch sie die Zweckerreichung zumindest gefördert wird[21].

Ebenso wie der EuGH geht das BVerfG daher von der Nützlichkeit der Vorratsdatenspeicherung für die Bekämpfung von Kriminalität aus, anders als der EuGH bejaht es aber auch deren Erforderlichkeit per se. Beide Gerichte sind sich jedoch einig darin, dass ein Zusammenhang

---

13 vgl. Urteil des EuGH, aaO, Rdnr. 56 und 59

14 vgl. Urteil des EuGH, aaO, Rdnr. 58

15 vgl. BVerfGE 125, 260 ff

16 vgl. BVerfGE, aaO, S. 316 ff

17 vgl. BVerfGE, aaO, S. 317

18 vgl. BVerfGE, aaO, S. 318

19 vgl. dazu im Einzelnen BVerfGE, aaO, S. 325 ff

20 vgl. BVerfGE, aaO, S. 321

21 vgl. BVerfGE, aaO, S. 317f mit Hinweis auf BVerfGE 63, 88[115]; 67, 157[175]; 96, 10[23]; 103, 293[307]

zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit bestehen muss[22], bzw. dieser Zusammenhang mindestens durch die Förderung der Zweckerreichung[23] hergestellt wird.

4) Anlasslose Speicherung zulässig?

Einen Nachweis über einen Zusammenhang zwischen der anlasslosen Vorratsdatenspeicherung und der Bekämpfung von Kriminalität enthält der vorliegende Gesetzesentwurf nicht. Er nimmt auch nicht substantiiert dazu Stellung, ob und inwiefern der verfolgte Zweck durch das Gesetz gefördert wird.

Der Entwurf äußert sich zudem nur an wenigen Stellen und sehr allgemein zur Erforderlichkeit der Gesetzgebung. So wird nur abstrakt ausgeführt, dass die Einführung einer gesetzlichen Pflicht zur Speicherung von Verkehrsdaten durch die Erbringer öffentlich zugänglicher Telekommunikationsdienste erforderlich sei, um Lücken der Strafverfolgung und der Gefahrenabwehr im Einzelfall zu schließen und damit dem verfassungsrechtlichen Gebot einer effektiven Strafverfolgung zu genügen[24]. Zudem werden „Unzulänglichkeiten bei der Strafverfolgung und der Gefahrenabwehr“[25] sowie Urteile des EGMR[26] und des EuGH[27] zur Begründung der Notwendigkeit des Gesetzes angeführt.

Diese undifferenzierte und damit pauschale Begründung vermag die Erforderlichkeit der Vorratsdatenspeicherung nicht zu rechtfertigen. Der Gesetzgeber muss auf der Grundlage ihm vorliegender Daten nachvollziehbar darlegen, aus welchen Gründen und in welcher Weise er Maßnahmen trifft, wenn er - wie vorliegend - einen Einschätzungs- und Beurteilungsspielraum in Anspruch nimmt[28].

---

22 vgl. EuGH, aaO, Rdnr. 59

23 vgl. die Rspr. bei Fn 21

24 vgl. Regierungsentwurf, S. 1

25 vgl. Regierungsentwurf, S. 22

26 vgl. Regierungsentwurf, aaO, Urteil des EGMR, Nr. 2872/02 vom 2. Dezember 2008 (- K.U. v. Finnland), wonach positive Pflichten für die Staaten bestehen, das materielle Strafrecht in der Praxis durch effektive Ermittlung und Verfolgung anzuwenden

27 vgl. aaO, Urteil des EuGH in Sachen Digital Rights, Az: C-293/12 und C-564/12, Rdnr. 42, allerdings unterlässt es die Begründung im Regierungsentwurf, darauf hinzuweisen, dass der EuGH an anderer Stelle sehr deutlich die Erforderlichkeit von Speicherungsmaßnahmen für die Kriminalitätsbekämpfung verneint, siehe Rdnr. 51

28 vgl. BVerfGE 79, 311 (344)

Das Max-Planck-Institut für ausländisches und internationales Strafrecht (MPI) hat in einem 2011 veröffentlichtem Gutachten zu „Schutzlücken durch Wegfall der Vorratsdatenspeicherung?“[29] dargelegt, dass „die Aufklärungsquote in Deutschland in keinem Fall unter den für die Schweiz mitgeteilten Aufklärungsquoten liegt. Vielmehr liegen die Aufklärungsquoten teilweise deutlich höher. Dies gilt auch für solche Delikte, für die die besondere Bedeutung des Zugriffs auf Telekommunikationsverkehrsdaten hervorgehoben wird (also Computerbetrug, Verbreitung von Pornografie (einschließlich Kinderpornografie) oder Drohung).“[30] Relevant ist dieses Ergebnis deswegen, weil in der Schweiz seit 2001 so genannte Randdaten der Telekommunikation auf Vorrat gespeichert werden, wobei diese Daten die Obergruppe zu den Verkehrsdaten darstellen, die hier in Rede stehen.[31]

In dem Gutachten, dem außer eigenen Erhebungen auch Interviews mit Praktikern aus der Strafverfolgung zu Grunde liegen, kommt das MPI im Übrigen zu dem Ergebnis, dass geeignete, belastbare Daten, die zu einer quantitativen Überprüfung der Auswirkungen der Vorratsdatenspeicherung auf die Aufklärungsquote führen könnten, bislang nicht erfasst werden und auch nicht systematisch erfasst werden sollen. Die auf Einzelfälle gegründete Argumentation zugunsten der Vorratsdatenspeicherung weise den Einzelfall als „typisch“ aus, ohne dass diese Einordnung empirisch belegt oder belegbar wäre[32].

Zu einem vergleichbaren Ergebnis kommt der wissenschaftliche Dienst des Bundestages in einem Rechtsgutachten aus dem Jahr 2011. Darin wird auf der Grundlage von Zahlen des BKA eine Steigerung der Aufklärungsquote um sechs/Tausendstel Prozent angegeben, wenn die Vorratsdatenspeicherung angewandt wird[33].

Die polizeiliche Kriminalitätsstatistik zeigt zudem auf, dass in den Deliktsgruppen, in denen die Relevanz der Telekommunikationsverkehrsdaten bzw. der Zugriff auf diese besonders betont wird, in den letzten Jahren 2014 und 2013 keine signifikant schlechteren Aufklärungsquoten ausgewiesen werden[34].

---

29 vgl. https://www.mpg.de/5000721/vorratsdatenspeicherung.pdf; vgl. dazu auch BT-Drs. 18/4971

30 vgl. Fn. 29, aaO, S. 123

31 vgl. dazu https://de.wikipedia.org/wiki/Randdaten_%28bei_der_Nutzung_elektronischer_Infrastruktur%29

32 vgl. Gutachten MPI, S. 218 (219)

33 vgl. Rechtsgutachten des wissenschaftlichen Dienstes des Deutschen Bundestages vom 25.02.2011, S.20 WD 11-3000-18/11, mit Berufung auf: Gietl, Die Einführung der Vorratsdatenspeicherung, K&R 2007, S. 545-550 (552)

34 vgl. www.bka.de, Publikationen/Polizeiliche Kriminalstatistik

Nach alledem besteht erheblicher Zweifel daran, dass die vorgesehene Gesetzgebung zur Einführung der Vorratsdatenspeicherung auch nur die Möglichkeit bietet, die verfolgte Zielsetzung der effektiven Bekämpfung der Kriminalität zu fördern. Jedenfalls aber ist ein Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit nicht erkennbar. Es ist daher auch nicht verwunderlich, dass sich die Bundesregierung in ihrem Gesetzentwurf nicht mit den (wenigen) vorliegenden Daten auseinandersetzt, sondern sich in allgemeine Aussagen über angebliche Strafbarkeits- und Gefahrenabwehrlücken flüchtet.

III. Zu einzelnen Regelungen des Gesetzentwurfs

1) Schutz der Berufsgeheimnisse, § 100g Abs. 4 StPO-E

Der Gesetzentwurf will durch § 100g Abs. 4 StPO ein grundsätzliches Verbot der Erhebung von Verkehrsdaten regeln, die sich gegen die in § 53 Abs. 1 Nr. 1 bis 5 StPO genannten Personen richtet. Da es nicht möglich sei, die Berufsgeheimnisträger in ihrer Gesamtheit schon von der Speicherung ihrer Verkehrsdaten auszunehmen, zumal diese „in vielen Fällen nicht über statische, sondern über dynamische IP-Adressen" verfügten, ergebe sich der „bessere Schutz" durch eine Regelung, die die Verwendung der gespeicherten Daten ausschließe. Dieser Schutzmechanismus habe sich in der StPO auch an anderer Stelle bewährt[35].

Mit der Vorschrift des § 100g Abs. 4 StPO knüpft der Entwurf an die Regelung des § 160a StPO an. Anders als § 160a StPO unterscheidet § 100g Abs. 4 StPO-E jedoch nicht zwischen den verschiedenen Gruppen der Berufsgeheimnisträger nach § 53 StPO[36]. Das ist zu begrüßen, ändert jedoch nichts an der grundsätzlichen Kritik der hier Stellung nehmenden Organisationen[37] auch an dieser Vorschrift, insbesondere an § 160a Abs. 2 StPO. Die Norm bietet nämlich entgegen der Annahme der Bundesregierung[38] keinen ausreichenden Schutz davor, mit Hilfe staatlicher Maßnahmen die Person des Informanten zu ermitteln.

Verkehrsdaten haben nach der Rechtsprechung des Bundesverfassungsgerichts[39] einen besonders schutzwürdigen Aussagegehalt, weil sie im Einzelfall erhebliche Rückschlüsse auf das Kommunikations- und Bewegungsverhalten der Telekommunikationsnutzer zulassen. Deren

---

35 vgl. Regierungsentwurf, S. 37

36 vgl. Regierungsentwurf, aaO

37 vgl. Rechtsausschuss des Deutschen Bundestages, öffentliche Anhörung am 26.01.2011: Stellungnahme von ARD, BDZV, DJV, Deutscher Presserat, VDZ, Ver.di, VPRT und ZDF vom 19.01.2011, S. 23ff

38 vgl. BT-Drs. 16/11170, S. 5

39 BVerfG AfP 2003, 138 (143); BVerfG NJW 2006, 976 (980 f.); BVerfGE 125, 260 (319)

Speicherung für Strafverfolgungszwecke und der staatliche Zugriff können in der Folge die Unbefangenheit des Kommunikationsaustausches und das Vertrauen in den Schutz der Unzugänglichkeit der Telekommunikationsanlagen zunehmend gefährden[40] bzw. ein Gefühl der Überwachung erzeugen, das mit dem Menschenwürdebild des Grundgesetzes unvereinbar ist.

Der den Verkehrsdaten der Telekommunikation zugeschriebene Aussagegehalt trifft alle Telekommunikationsvorgänge, insbesondere auch die Telekommunikation zwischen Journalistinnen und Journalisten und ihren Informantinnen und Informanten bzw. die berufliche Telekommunikation untereinander. Die berufliche Kommunikation von Journalistinnen und Journalisten wird im Hinblick auf Telekommunikationsvorgänge nicht nur durch Art. 5 Abs. 1 S. 2 GG, sondern auch durch Art. 10 Abs. 1 GG geschützt[41].

Nach der ständigen Rechtsprechung sowohl des Bundesverfassungsgerichts, wie auch des Bundesgerichtshofs ist die Ausforschung der die Informanten schützenden Daten[42] nicht zulässig[43]. Der Schutz der Informanten umfasst nach dieser Rechtsprechung nicht nur den Inhalt der Mitteilung und den Namen des Informanten, sondern auch alle Umstände, aus denen sich eine Identifikation von Informanten ergeben könnte. Ausdrücklich wird dies in § 53 Abs. 2 S. 3 StPO seit 2002 gesetzlich geregelt. Danach kann der Zeuge auch in ansonsten der Zeugnispflicht unterliegenden Fällen die Aussage verweigern, soweit sie „zur Offenbarung der Person des Verfassers oder Einsenders (…) oder des sonstigen Informanten" führen würde. Sowohl die Rechtsprechung wie auch die zitierte gesetzliche Regelung wird damit begründet, dass es mit Art. 5 Abs. 1 S. 2 GG nicht vereinbar sei, wenn der Schutz journalistischer Quellen sich lediglich auf den Inhalt der gemachten Mitteilung beziehe, nicht aber auf die Umstände, die zur Identifikation des Informanten führen. Müssten solche Umstände offenbart werden, würde die Presse- und Rundfunkfreiheit bei nicht öffentlich zugänglichen sensiblen Materien leer laufen, denn kaum ein Informant würde sich ohne Wahrung der Vertraulichkeit dem Risiko seiner Identifikation und eventuellen Maßregelung aussetzen. Die Pressefreiheit als Institution würde Schaden nehmen.[44] Dies widerspricht der ständigen Rechtsprechung des Bundesverfassungsgerichtes.

Nichts anderes kann gelten, wenn mit Hilfe von Verkehrsdaten das Kommunikations- und Bewegungsverhalten von Journalistinnen und Journalisten und ihrer potenziellen Informanten auf

---

[40] BVerfGE 100, 313 (381); BVerfGE 125, 260 (310); EuGH, aaO (Fn. 1), Rdnr. 66

[41] BVerfGE 107, 299; OLG Dresden AfP, 2007, 577 (578)

[42] z.B. Umstände von Treffen mit Informanten, ggf. Zahlungsbeträge, Örtlichkeiten, Zeiten usw.

[43] vgl. BVerfG, NStZ 1982, 253 (254); BGH NJW 1990, 525 (526) m.w.N.

[44] vgl. Achenbach, in: Löffler, Presserecht, 5. Aufl. 2006, § 23 LPG, Rdnr. 25.

Vorrat gespeichert werden soll, um bei Bedarf auf diese Daten zugreifen zu können. Über Abgleiche von Bewegungsverhalten könnten zudem auch persönliche Treffen nachvollzogen werden.

Eine grundrechtlich geschützte Presse- und Rundfunkfreiheit kann nicht verwirklicht werden, wenn die ungehinderte Informationsbeschaffung und eine vertrauliche Kommunikation der Medien insbesondere mit den Informanten nicht mehr möglich sind. Potenzielle Informanten würden ihre Kenntnisse nicht weiter geben, wenn sie sich nicht darauf verlassen könnten, dass die Journalistinnen und Journalisten ihre Quellen nicht preisgeben. Es geht dabei nicht ausschließlich um den Schutz der Quellen, sondern auch um den Schutz des Redaktionsgeheimnisses, dem das BVerfG in ständiger Rechtsprechung eigenständige Bedeutung zumisst und in das eingegriffen würde, wenn die im Bereich journalistischer Recherche hergestellten Kontakte staatlich ausgeforscht würden[45] oder nachvollzogen werden können.

Die für den öffentlichen Meinungsbildungsprozess wichtige Aufgabe der Journalistinnen und Journalisten, Missstände an die Öffentlichkeit zu bringen, ist massiv gefährdet, wenn Informanten befürchten müssen, dass ihre Informationen nicht vertraulich bleiben, sondern z.B. durch die Herausgabe von Verkehrsdaten etc. personalisiert werden können. Dasselbe gilt, wenn Journalistinnen und Journalisten zudem damit rechnen müssten, dass ihre Kontakte staatlicherseits ausgeforscht werden können.

Das Bundesverfassungsgericht hat es in seinem Urteil zur Vorratsdatenspeicherung verfassungsrechtlich für geboten erachtet, zumindest für einen engen Kreis von auf besondere Vertraulichkeit angewiesenen Telekommunikationsverbindungen ein grundsätzliches Übermittlungsverbot vorzusehen[46]. Begründet hat es diese Rechtsprechung mit der notwendigen Einhaltung des Verhältnismäßigkeitsgrundsatzes. Es hat dabei nicht ausdrücklich alle Gruppen von Berufsgeheimnisträger(innen) im Sinne des § 53 StPO erwähnt, sondern als Beispiel für auf besondere Vertraulichkeit Angewiesene auf seelsorgerische Tätigkeiten im Hinblick auf die Regelung in § 99 Abs. 2 TKG abgestellt. Deren Daten dürfen jedenfalls an staatliche Stellen nicht übermittelt werden, wenn sie sich bei der Bundesnetz-Agentur haben registrieren lassen, § 113b Abs. 6 TKG-E. Eine solche Registrierung kommt jedoch für Journalistinnen und Journalisten nicht in Betracht, sie würde ihrerseits gegen Art. 5 Abs. 1 S. 2 GG verstoßen[47]. Aus diesem Umstand kann allerdings nicht der Schluss gezogen werden, dann komme nur noch ein

---

[45] vgl. BVerfGE 117, 244 (259) mit Hinweis auf BVerfGE 66, 116 (133 ff); 107, 299 (331)

[46] vgl. BVerfGE 125, 260 (334)

[47] Die Ausübung des journalistischen Berufs kann von einer „wie immer gearteten Berufszulassung" nicht abhängig gemacht werden, Degenhart; Bonner Kommentar GG, Rdnr. 441, 122. Aktualisierung, 2006

Verwertungsverbot in Betracht, wie es grundsätzlich in § 100g Abs. 4 StPO-E vorgesehen[48] ist, denn bereits die Erhebung und Speicherung ist geeignet, Vertrauensverhältnisse zu unterbinden. Die Bereichsausnahme für den journalistischen Bereich muss daher bereits bei der Datenspeicherung ansetzen.

Wenn das BVerfG mindestens ein Übermittlungsverbot für auf besondere Vertraulichkeit angewiesene Telekommunikationsverbindungen als verfassungsrechtlich geboten erachtet, kann ein Verwertungsverbot allein diesen Anforderungen nicht genügen, denn es setzt die Übermittlung voraus. Genügt daher ein Verwertungsverbot den Anforderungen nicht und kommt ein Übermittlungsverbot rechtlich und tatsächlich nicht in Betracht, muss schon die Speicherung der besonders zu schützenden Telekommunikationsverbindungen unterbleiben. Diese Konsequenz hat der EuGH[49]ebenfalls aufgezeigt.

Die Notwendigkeit des Schutzes der Berufsgeheimnisträger wird vom EuGH in der Entscheidung zur Richtlinie 2006/24/EG generell höher eingestuft, als nach dem Urteil des Bundesverfassungsgerichts zur Vorratsdatenspeicherung. Hinsichtlich der Frage, ob der mit einer Vorratsdatenspeicherung verbundene Eingriff in die Rechte aus Artikel 7 und Artikel 8 der Charta auf das absolut Notwendige beschränkt ist, hat der EuGH nicht nur moniert, dass die anlasslose Vorratsdatenspeicherung unterschiedslos alle Personen betrifft, die elektronische Kommunikationsmittel benutzen. Er hat vor allem auch kritisch angemerkt, dass nach der Richtlinie 2006/24/EG keinerlei Ausnahme für Personen vorgesehen war, deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen[50].

Die Notwendigkeit des Schutzes gerade der journalistischen Arbeit und des dafür essentiellen Quellenschutzes wird auch durch die Rechtsprechung des EGMR unterstrichen. Der Schutz der journalistischen Quellen ist danach von vitaler Bedeutung für die Pressefreiheit[51]. Er wird als eine der Grundvoraussetzungen der Pressefreiheit angesehen. Potenzielle Quellen ohne diesen Schutz könnten davon abgehalten werden, die Presse dabei zu unterstützen, die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse zu informieren. Der Gerichtshof betont, dass ohne den Schutz der Quellen eines Journalisten die wichtige öffentliche Kontrollfunktion der Presse untergraben werden könnte und die Fähigkeit der Presse, genaue und verlässliche Informationen zu liefern, negativ beeinflusst werden könnte[52]. Eine Anordnung zur Preisgabe von Quellen könne nicht nur eine nachteilige Wirkung auf die Quelle selbst haben, sondern auch

---

48 vgl. die Position der Bundesregierung, Fn. 35

49 vgl. EuGH, Fn. 1, Rdnr. 59

50 vgl. EuGH, aaO, Rdnr. 58

51 vgl. EGMR, Case of Sanoma Uitgevers B.V. v. The Netherlands, no. 38224/04, judgm. 14/09/2010, Rdnr. 88

52 vgl. EGMR, Case of Goodwin v. The United Kingdom, no. 17488/90, judgment 27/03/1996, Rdnr. 39

z. B. auf die Zeitung oder den Sender, deren Glaubwürdigkeit dadurch in Gefahr gerate, und auf die Öffentlichkeit, die ein Interesse daran habe, Informationen zu erhalten, die (auch) aus anonymen Quellen stammten[53]. Das gilt auch dann, wenn eine Information öffentlich eingeholt wurde und keine besondere Geheimhaltungspflicht besteht. Ein Eingriff in den Informantenschutz sei bereits in der Aufforderung einer Behörde zu sehen, die Quelle preis zu geben[54]. Auch wenn eine Anordnung nicht vollstreckt wird, ist sie als Verstoß gegen den durch Art. 10 EMRK geschützten Quellenschutz zu qualifizieren, wenn damit bezweckt werden soll, dass die Identität einer anonymen Quelle offen zu legen ist[55].

Die überragende Bedeutung, die der Presse- und Rundfunkfreiheit für das Gemeinwesen und die Demokratie zukommt und die ohne Quellenschutz und den Schutz des Redaktionsgeheimnisses nicht auskommen, sowie die Anforderung des EuGH, Telekommunikationsverbindungen der Berufsgeheimnisträger bereits aus der Speicherpflicht herauszunehmen und schließlich der Hinweis des BVerfG, die Daten von besonders auf Vertraulichkeit angewiesene Telekommunikationsverbindungen mindestens nicht zu übermitteln, lassen nach Ansicht der Stellung nehmenden Organisationen nur den Schluss zu, dass die Erhebung und Speicherung insgesamt zu unterbleiben hat. Jedenfalls dürfte die vorgeschlagene Regelung zu § 100g Abs. 4 StPO, die lediglich ein Verwertungsverbot vorsieht, mit der Rechtsprechung des EuGH wie dargestellt, nicht vereinbar sein.

§ 100g Abs. 4 StPO stellt hinsichtlich des Schutzes der Berufsgeheimnisträger vor einer Verwertung ihrer Verkehrsdaten darauf ab, dass die Erhebung von Verkehrsdaten nach Absatz 2 unzulässig ist, wenn sie sich gegen eine der in § 53 Abs. 1 S. 1 Nr. 1 bis 5 StPO genannten Personen richtet und sie voraussichtlich Erkenntnisse erbringen würde, über die diese Personen das Zeugnis verweigern dürften. Die Formulierungen „die voraussichtlich Erkenntnisse erbringen würde" sowie „diese das Zeugnis verweigern dürfte" sind ersichtlich aus § 160a StPO übernommen worden. Dafür spricht auch, dass nach § 100g Abs. 4 S. 6, § 160a Abs. 3 und 4 entsprechend gelten sollen.

Damit kommt die Bundesregierung den Anforderungen des BVerfG[56] scheinbar nach, besonders auf Vertraulichkeit angewiesene Telekommunikationsverbindungen weitergehend zu schützen. Jedoch ist dieser Schutz bei näherer Betrachtung als Einzelfallregelung ausgestaltet und führt somit keineswegs zu einem generellen Schutz vor der Auswertung und Verwendung

---

[53] vgl. EGMR, Case of Sanoma Uitgevers B.V. v. The Netherlands, no. 38224/04, aaO, Rdnr. 89

[54] vgl. EGMR, British Broadcasting Corporation v. The United Kingdom, no. 25798/94, judgment 18/01/1996, 4

[55] vgl. EGMR, Financial Times Ltd. v. The United Kingdom, no. 821/03, judgment 15/12/2009, Rdnr. 70

[56] vgl. BVerfGE 125, 260 (334)

der gespeicherten Daten. Die Unzulässigkeit der Erhebung bzw. des Abrufes durch die berechtigte Behörde nach § 100g Abs. 4 StPO setzt nämlich voraus, dass die Maßnahme sich gegen eine zeugnisverweigerungsberechtigte Person richtet ***und*** voraussichtlich Erkenntnisse erbringen würde, über die eine Journalistin oder ein Journalist das Zeugnis verweigern dürfte, oder dass sie sich zwar nicht gegen eine solche Person richtet, gleichwohl aber Erkenntnisse erlangt werden, über die eine zeugnisverweigerungsberechtigte Person keine Aussage machen bräuchte.

Diese Regelung ist im Hinblick auf die Tragweite und die Anwendung der Übermittlung bzw. des Abrufs der damit zusammenhängenden Verkehrsdaten weder klar noch präzise im Sinne des Urteils des EuGH[57]. Einen wirksamen Schutz vor der Übermittlung bzw. dem Abruf von Verkehrsdaten von Journalistinnen und Journalisten bietet die Regelung jedenfalls nicht.

Mit den gewählten Formulierungen sind zudem Prognoseentscheidungen verbunden, nämlich die, ob der Adressat des Verkehrsdatenabrufs ein Berufsgeheimnisträger ist bzw. ein solcher in die Ermittlungsmaßnahme involviert ist und ob der Abruf der Verkehrsdaten voraussichtlich Erkenntnisse zu Tage fördern würde oder erbringt, die in den Schutzbereich des Berufsgeheimnisses fallen würden. Mag die Identifizierung einer Person als Berufsgeheimnisträger in vielen oder sogar den meisten Fällen noch ohne großen Aufwand möglich sein, ist die Prognose, ob zur Verweigerung des Zeugnis berechtigende Erkenntnisse erlangt würden, ohne Kenntnis der Verkehrsdaten kaum möglich. Oder anders gewendet: beantragende Behörden müssten im Regelfall davon ausgehen, dass die Verkehrsdaten, die sie erheben wollen, keine die Zeugnisverweigerung betreffenden Erkenntnisse erbringen.

Mit den gleichen Prognosevoraussetzungen haben es Behörden und Gerichte bei der Anwendung des § 160a StPO zu tun. Zu dieser Vorschrift wird davon ausgegangen, dass „nur dann ex ante von der Unzulässigkeit der Maßnahme auszugehen (ist), wenn ausreichende äußere Anzeichen, also konkrete tatsächliche Anhaltspunkte, vorliegen, dass (…) geschützte Erkenntnisse zu erwarten sind."[58] M.a.W. liegen solche Anhaltspunkte nicht vor, ist von der Zulässigkeit der Maßnahme auszugehen, denn die Erhebung ist danach nur unzulässig, wenn „zweifelsfrei erkannt wird, dass schutzrelevante Inhalte Gegenstand der Erhebung sind."[59]

Angesichts der mit den in § 100g Abs. 4 StPO-E verwendeten Formulierungen und den damit verbundenen Schwierigkeiten, zweifelsfrei zu erkennen, ob schutzrelevante Erkenntnisse mit

---

[57] vgl. Urteil des EuGH, aaO, Rdnr. 54

[58] vgl. KK-StPO/Griesbaum, StPO, § 160a Rdnr. 6, 7. Auflage 2013

[59] vgl. KK-StPO, aaO, Rdnr. 6

dem Abruf der Verkehrsdaten verbunden sein würden oder auch, ob der Adressat eine Journalistin oder ein Journalist ist, muss davon ausgegangen werden, dass Strafverfolgungsbehörden auch bei § 100g Abs. 4 StPO-E - bei Vorliegen der übrigen Voraussetzungen der Erhebung - grundsätzlich die Zulässigkeit des Abrufs von Verkehrsdaten bei Berufsgeheimnisträgern annehmen würden.

Auch hinsichtlich des der unzulässigen Erhebung nachgelagerten Verwendungs- bzw. Verwertungsverbots muss angenommen werden, dass dieses wie bei § 160a StPO nur dann zum Zuge kommen soll, wenn sich „zweifelsfreie Hinweise ergeben, dass geschützte Erkenntnisse anfallen oder angefallen sind."[60]

Der vermeintliche Schutz der Berufsgeheimnisträger nach § 100g Abs. 4 erweist sich damit im Hinblick auf den Abruf der Verkehrsdaten und möglicherweise ihre weitere Verwendung als weitgehend wirkungslos. Berufsgeheimnisträger sind dem Entwurf nach vor der Speicherung der Verkehrsdaten nicht und vor deren Erhebung nur dann geschützt, wenn und solange Strafverfolgungsbehörden und Ermittlungsgerichte nicht aufgrund fehlender zweifelsfreier Erkenntnisse von der grundsätzlichen Zulässigkeit des Abrufs der Verkehrsdaten ausgehen können. Dabei tritt der Umstand hinzu, dass Strafverfolgungsbehörden nicht verpflichtet sind, für die zu erstellende Prognose besondere Ermittlungen durchzuführen[61].

Es ist für die an dieser Stellungnahme beteiligten Medienunternehmen und -verbände unverständlich, warum der Gesetzesentwurf auf jegliche Anstrengung verzichtet, den Schutz der Berufsgeheimnisträger - wie rechtlich geboten - bereits auf der Ebene der Speicherung vorzunehmen. Dies alleine, wie der Gesetzesgründung zu entnehmen ist, mit der Feststellung abzutun „Die Berufsgeheimnisträger in ihrer Gesamtheit schon von der Speicherung ihrer Verkehrsdaten auszunehmen, ist nicht möglich."[62] geht sowohl an den praktischen Gegebenheiten als auch an der rechtlichen Ausgangslage, nämlich der Pflicht des Gesetzgebers zu genau solchen Anstrengungen, vorbei.

Für die Sendeanstalten und -unternehmen, die Verlagshäuser und andere Institutionen des Medienbereichs und damit für deren Beschäftigte stehen sowohl die IP-Nummernkreise als auch die Festnetztelefonnummern und in vielen Fällen auch die dienstlichen Mobilfunknummern fest. Sie sind bereits heute den TK-Providern als Bestandsdaten speziell von Medienunternehmen und Journalistinnen und Journalisten bekannt. Aus diesem Grunde wäre eine Regelung

---

[60] vgl. KK-StPO, aaO, Rdnr. 7

[61] vgl. KK-StPO, aaO, Rdnr. 6

[62] vgl. Regierungsentwurf, S. 37

geboten, für diese Anschlüsse auf die Speicherung der Verkehrsdaten zu verzichten. Eine Registrierung bei der Bundesnetzagentur, wie sie § 99 Abs. 2 des Telekommunikationsgesetzes (TKG) für die Seelsorge und die Beratungsstellen vorsieht, wäre, da es hier nur auf die Kenntnis der TK-Provider ankommt, entbehrlich. Diese Registrierung wäre (s.o.) als Verstoß gegen Art. 5 Abs. 1 S. 2 GG auch unzulässig.

Insgesamt ist es höchst zweifelhaft, ob die bislang vorgesehene Regelung mit der vom Bundesverfassungsgericht festgestellten Ausprägung des Verhältnismäßigkeitsgrundsatzes vereinbar ist, wonach bereits ein Übermittlungsverbot von durch die Vorratsdatenspeicherung gewonnen Daten für einen engen Kreis von auf besondere Vertraulichkeit angewiesene Berufsgeheimnisträger gilt. Mit der Rechtsprechung des EuGH zum Verhältnis von Berufsgeheimnis und Vorratsdatenspeicherung ist die vorgeschlagene Schutzregelung nicht in Einklang zu bringen.

Problematisch ist die Regelung vor allem aber auch hinsichtlich der Personen, um deren Willen Journalistinnen und Journalisten ein Zeugnisverweigerungsrecht haben. Das Verbot der Erhebung der Verkehrsdaten bzw. das Verbot des Abrufs geht ins Leere, wenn Adressat dieser Maßnahme nicht die Journalistin oder der Journalist ist, sondern die potenzielle Informantin bzw. der potenzielle Informant. Staatliche Stellen können sich insoweit trotz der Regelung in § 100g Abs. 4 StPO dann Einblick in die journalistische Arbeit verschaffen, wenn der Abruf beim vermuteten Informanten erfolgt.

2) Zu § 101a StPO-E

In § 101a Abs. 1 wird der für Verkehrsdatenerhebungen nach § 100g wesentliche Richtervorbehalt geregelt. Hierbei wird nach der Art der gespeicherten Daten differenziert. Durch die Vorschrift des Abs. 1 S. 2 werden für die Fälle des § 100g Abs. 2, auch in Verbindung mit § 100g Abs. 3 S. 2, die § 100b Abs. 1 S. 2 und 3 von der Anwendung ausgenommen. Damit ist zwar sichergestellt, dass für die Erhebung der auf Vorrat zu speichernden Daten die Möglichkeit einer Eilanordnung durch die Staatsanwaltschaft bei Gefahr im Verzug nicht gegeben ist; aber es bleibt hinsichtlich des Richtervorbehalts bei der Regelung in Absatz 1 Satz 1. Danach ist eine Eilanordnung im Falle des § 100g Abs. 1 nach wie vor zulässig, weil wie bisher auf § 100a Abs. 3 und § 100b Abs. 1 bis 4 StPO verwiesen wird.

Auch insoweit ist zu konstatieren, dass der Schutz der Berufsgeheimnisträger und Berufsgeheimnisträgerinnen höchst unvollkommen ausgestaltet wird. Nicht nur unterliegen sie hinsichtlich der von ihnen geheim zuhaltenden Tatsachen nur dem Schutz einer Verhältnismäßigkeitsprüfung, auch der Richtervorbehalt ist nicht so konstruiert, dass er nicht umgegangen werden

könnte. So ist es für die Strafverfolgungsbehörden über den Weg des § 100g Abs. 1 ohne weiteres möglich, Verkehrsdaten nach § 96 TKG zu erheben. Diese sind denen durchaus vergleichbar, die nach § 113b Abs. 2 TKG-E gespeichert werden müssen. Der Schutz der Berufsgeheimnisse, vor allem aber der Informantenschutz und das Redaktionsgeheimnis erfordern es jedoch, den Richtervorbehalt ohne Ausnahme zu gewährleisten.

Unter den notwendigen Verfahrensgarantien einer Rechtsordnung ist zuerst und vor allem die Garantie notwendig, dass ein Richter oder eine unabhängige und unparteiische Stelle angerufen werden kann, bevor die Polizei oder der Staatsanwalt Zugang zu den (journalistischen) Quellen erhält[63]. Obwohl auch die Staatsanwaltschaft an Recht und Gesetz gebunden ist[64], stellt sie doch, was das Ermittlungsverfahren anbelangt, eine „Partei" dar, die Interessen vertritt, die möglicherweise nicht mit dem journalistischen Quellenschutz vereinbar sind[65]. Sie kann daher wohl kaum als objektive und unparteiische Partei angesehen werden, von der erwartet werden kann, dass sie die angemessene Bewertung der konkurrierenden Interessen vornimmt.

3) Zu Art. 5, § 202d StGB

Nach der geplanten neuen Vorschrift des § 202d StGB soll strafbar handeln, wer Daten, die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen.

Der Straftatbestand soll nicht öffentlich zugängliche, elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeicherte Daten erfassen. Er soll das formelle Datengeheimnis schützen. Als Vortat einer Datenhehlerei sollen alle Taten in Betracht kommen, die ein Strafgesetz verwirklichen, unabhängig von der Schuld des Täters oder vom Vorliegen eines Strafantrages, z.B. das Abfangen und Ausspähen von Daten (§§ 202a, 202b StGB), Diebstahl (§ 242

---

[63] vgl. EGMR (Fn.51); Case of Sanoma Uitgevers B.V. v. The Netherlands, Rdnr. 90: "First and foremost among these safeguards is the guarantee of review by a judge or other independent and impartial decision-making body."

[64] vgl. EGMR, Case of Sanoma Uitgevers B.V. v. The Netherlands, Rz. 93: "Although the public prosecutor, like any public official, is bound by requirements of basic integrity, in terms of procedure he or she is a "party" defending interests potentially incompatible with journalistic source protection and can hardly be seen as objective and impartial so as to make the necessary assessment of the various competing interests."

[65] vgl. Fn 63. Der entsprechende Ermittlungseifer der Staatsanwaltschaft war jüngst bei den unbegründeten Ermittlungen wegen angeblichen Landesverrats gegen netzpolitik.org und Journalisten dieses Mediums zu besichtigen.

StGB), Betrug (§ 263 StGB), Computerbetrug (§ 263a StGB), Nötigung (§ 240 StGB), Fälschung technischer Aufzeichnungen (§ 269 StGB) etc.[66]

§ 202d Abs. 3 StGB sieht einen Tatbestandsausschluss für Handlungen vor, die ausschließlich zu dem Zwecke der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Dazu sollen, als von beruflichen Pflichten umfasst, auch journalistische Tätigkeiten in Vorbereitung einer konkreten Veröffentlichung gehören[67]. Durch das Ausschließlichkeitskriterium soll entsprechend der Regelung des § 184b Abs. 5 StGB sichergestellt werden, dass die konkrete Aufgabenerfüllung einziger Grund für die Verwendung der Daten ist[68].

Im Einzelnen sollen nach § 202d Abs. 3 S. 2 StGB-E solche beruflichen Handlungen der in § 53 Abs. 1 S. 1 Nr. 5 der Strafprozessordnung genannten Personen von der Anwendung des Tatbestandes ausgeschlossen sein, mit denen Daten entgegengenommen, ausgewertet oder veröffentlicht werden. Dabei soll § 202d Abs. 3 S. 2 StGB-E einen Unterfall des § 202d Abs. 3 S. 1 StGB-E darstellen[69]. § 202d Abs. 3 Satz 2 StGB-E ist im Wortlaut an § 353b Abs. 3a StGB angelehnt.

Gegenüber der Fassung des Referentenentwurfs wird nun bereits im Wortlaut des § 202d klargestellt, dass journalistische Tätigkeiten, die im Zusammenhang mit einer Datenhehlerei stehen könnten, nicht strafbar sind, wenn sie sich darin erschöpfen, Daten entgegenzunehmen, auszuwerten oder zu veröffentlichen. In der Begründung des Regierungsentwurfs wird allerdings auch darauf hingewiesen, dass wegen des gewählten Wortlautes die Auslegungsgrundsätze zu § 353b Abs. 3a StGB anzuwenden sind.

Demzufolge sollen auch bei § 202d StGB-E diejenigen Handlungen strafbar bleiben, die sich auf den Zeitraum beziehen, der vor der Vortat einer Datenhehlerei liegt oder in Zusammenhang mit der Vortat steht[70]. Es ist daher auch nach dem Wortlaut des Regierungsentwurfs nicht ausgeschlossen, dass eine Strafbarkeit wegen der journalistischen Tätigkeit angenommen wird, weil etwa vermutet wird, dass ein Journalist oder eine Journalistin durch seine bzw. ihre Tätigkeit nicht nur passiv die Vortat ermöglicht hat, sondern (z.B. durch eine vorherige Erklärung zur Entgegennahme oder zu einem Angebot einer Geldzahlung für die Daten) den Entschluss des Vortäters zur Tatbegehung auch aktiv gefördert oder vielleicht sogar hervorgerufen hat[71].

---

66 vgl. Regierungsentwurf, S. 54

67 vgl. zu der ähnlichen Formulierung in § 184b Abs. 5 StGB: MüKO/Hörnle, Rdnr. 41, 12. Auflage

68 vgl. Regierungsentwurf, S. 57; BT-Drs 12/4883, S. 8 f.

69 vgl. Regierungsentwurf, S. 57

70 vgl. zu § 353b Abs. 3a StGB: MüKo/Graf, § 353b, Rdnr. 58, 12. Aufl.

71 vgl. zu § 353b Abs. 3a StGB: Schönke/Schröder (Perron), § 353b, Rdnr. 21d, 29. Aufl.

Die Beschränkung des Schutzes der Journalistinnen und Journalisten auf in unmittelbarem Zusammenhang mit der (konkreten) Veröffentlichung stehenden Handlungen im Rahmen des § 202d StGB-E ist aber auch sachlich nicht gerechtfertigt. In solchen Handlungen erschöpft sich journalistische Tätigkeit nicht. Sollen tatsächlich nur solche journalistischen Tätigkeiten straffrei bleiben, die in „Vorbereitung einer **konkreten Veröffentlichung**" erfolgen[72]? Unklar ist schon, ob aus der ex-post-Betrachtung die Veröffentlichung konkret erfolgt sein muss oder ob von diesem Blickwinkel die Veröffentlichung konkret geplant sein muss. Und sollen umgekehrt z.B. vorgelagerte journalistische Tätigkeiten, vor allem Recherchen, die noch nicht mit geplanten konkreten Veröffentlichungen in Verbindung zu bringen sind, oder der Austausch von Rechercheergebnissen[73], der zwar auf Veröffentlichung gerichtet ist, zu dem aber eine konkrete Veröffentlichung noch nicht geplant ist, nach § 202d StGB-E ohne Ausnahme strafbar sein?

Das Ergebnis der geplanten Normen wäre eine Schwächung des Informantenschutzes und des Redaktionsgeheimnisses und damit eine erhebliche Beeinträchtigung der Presse- und Rundfunkfreiheit. Hinzu kommt, dass gerade im Ermittlungsverfahren die Strafverfolgungsbehörden etwa zum Zeitpunkt des Antrags auf Durchsuchung und Beschlagnahme - außer der Tatsache der Veröffentlichung - in aller Regel nicht mehr wissen, als dass ein Journalist oder eine Journalistin in die Datenhehlerei verwickelt sein könnte[74].

Es ist gerade eine Aufgabe der Medien und der Schutz des Art. 5 Abs. 1 S. 2 GG erstreckt sich deshalb darauf, Informationen zu beschaffen und Nachrichten und Meinungen zu verbreiten[75]. Allerdings gehören die Vorschriften des Strafgesetzbuches als allgemeine Gesetze zu den Schranken der Pressefreiheit des Art. 5 Abs. 2 GG. Die allgemeinen Gesetze sind ihrerseits im Licht der Pressefreiheit auszulegen und anzuwenden[76]. Die Einschränkung der Pressefreiheit muss geeignet und erforderlich sein, um den angestrebten Erfolg zu erreichen; dieser muss in

---

[72] So die Begründung, S. 57 mit Hinweis auf MüKo/Hörnle, aaO, der ebenso wenig wie der Regierungsentwurf erklärt, unter welchen Umständen eine „konkrete" Veröffentlichung anzunehmen ist.

[73] Man denke etwa an gemeinsame Recherchen verschiedener Medien.

[74] vgl. zu dem vergleichbaren Fall des Besitzes des gesuchten Materials: BVerfGE 117, 244 (246); auf dieses Problem hatten die Stellung nehmenden Organisationen schon im Gesetzgebungsverfahren zu § 353b StGB hingewiesen

[75] vgl. BVerfGE 10, 118 (121); 66, 116 (133); 77, 65 (74);
http://www.bverfg.de/entscheidungen/rk20101210_1bvr173904.html , Rz. 14

[76] vgl. BVerfGE 77, 65 (81ff); 107, 299 (329ff); BVerfG NJW 2001, 507; BVerfGE 117, 244 (261)

angemessenem Verhältnis zu den Einbußen stehen, welche die Beschränkung für die Pressefreiheit mit sich bringt[77]. Geboten ist insofern eine Abwägung zwischen dem sich auf die konkret zu verfolgenden Taten beziehenden Strafverfolgungsinteresse und der Pressefreiheit[78].

Gemessen daran stellt sich der Straftatbestand der Datenhehlerei als eine Störung dar, die das Potenzial einer einschüchternden Wirkung auf journalistische Quellen in sich trägt und damit als Beeinträchtigung der Presse- und Rundfunkfreiheit anzusehen ist[79].

Falls daher der Straftatbestand der Datenhehlerei eingeführt werden sollte, muss zweifelsfrei geregelt werden, dass journalistische Tätigkeiten vom Tatbestand generell nicht umfasst werden. § 202d Abs. 3 könnte demnach wie folgt formuliert werden:

„(3) Absatz 1 gilt nicht für Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Dazu gehören insbesondere

1. ....

2. berufliche Handlungen der in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Personen.“

Benno H. Pöppelmann
– DJV-Justiziar –

[77] vgl. BVerfGE 59, 231 (265); 71, 206 (214); 77, 65 (75)

[78] vgl. BVerfG NJW 2001, 507 (508)

[79] vgl. zu den Auswirkungen z.B. einer Durchsuchung: BVerfG NJW 2005, 965; BGH NJW 1999,2052 (2053); BVerfGE 117, 244 (259)

PRESSEMITTEILUNG

Vorratsdatenspeicherung beeinträchtigt Medienfreiheit

Berlin, 7.09.2015 – Die von der Bundesregierung geplante anlasslose Vorratsdatenspeicherung beeinträchtigt die Presse- und Rundfunkfreiheit. Sie schwächt den Informantenschutz und das Redaktionsgeheimnis. Zu diesem Schluss kommen die wichtigsten deutschen Medienverbände und -unternehmen in einer gemeinsamen Stellungnahme an die Abgeordneten des Deutschen Bundestags. Mit der Rechtsprechung des Europäischen Gerichtshofs seien die geplanten Regelungen nicht in Einklang zu bringen. Durch die Speicherung der Telekommunikationsdaten ließen sich die Kontakte zwischen Redaktionen und ihren Informanten nachvollziehen. Vorgesehen sei in dem Gesetz zur Vorratsdatenspeicherung zudem die Erhebung von Standortdaten, um Bewegungsprofile anfertigen zu können. „Jede Maßnahme für sich, aber auch deren Verknüpfung ist geeignet, das Vertrauen in den Informantenschutz nachhaltig zu untergraben bzw. gar nicht erst aufkommen zu lassen, was die journalistische Berichterstattungsfreiheit in nicht hinnehmbarem Maße gefährdet", heißt es in der Stellungnahme wörtlich.

Die Medienorganisationen DJV, dju in ver.di, BDZV, VDZ, VPRT, der Deutsche Presserat und die öffentlich-rechtlichen Sender ARD und ZDF fordern deshalb die Abgeordneten des Deutschen Bundestags auf, dem Gesetzentwurf zur Wiedereinführung der Vorratsdatenspeicherung die Zustimmung zu verweigern. Die 22-seitige Stellungnahme wurde am heutigen Montag an den Rechtsausschuss des Bundestags geschickt. Das Gremium wird sich voraussichtlich am 21. September mit der Vorratsdatenspeicherung befassen. In der Anhörung des Rechtsausschusses sollen nach derzeitiger Planung Vertreter der Medien nicht gehört werden.

Die Stellungnahme zur Vorratsdatenspeicherung ist auf den Online-Seiten der Medienverbände und -unternehmen zu finden.

DJV-Referat Presse- und Öffentlichkeitsarbeit:
Hendrik Zörner, Charlottenstr. 17, 10117 Berlin
Tel. (030) 72 62 79 2-0, E-Mail: djv@djv.de, www.djv.de

dju: Cornelia Haß, Paula-Thiede-Ufer 10, 10179 Berlin
Tel. (030) 69 56-23 22, E-Mail: dju@verdi.de, www.dju.verdi.de

BDZV: Anja Pasquay, Haus der Presse, Markgrafenstr. 15, 10969 Berlin
Tel. (030) 72 62 98-0, E-Mail: pasquay@bdzv.de, www.bdzv.de

VDZ: Peter Klotzki, Haus der Presse, Markgrafenstr. 15, 10969 Berlin
Tel. (030) 72 62 98-0, E-Mail: p.klotzki@vdz.de, www.vdz.de

PRESSEMITTEILUNG

Deutscher Presserat, Fritschestr. 27-28, 10585 Berlin
Tel. (030) 36 70 07-0, info@presserat.de, www.presserat.de

VPRT: Hartmut Schultz, Stromstr. 1, 10555 Berlin
Tel. (030) 39 88 8-0, E-Mail: info@vprt.de, www.vprt.de

ARD - Hessischer Rundfunk: Christoph Hammerschmidt, Bertramstraße 8, 60320 Frankfurt
Tel. (069) 155-0, E-Mail: christoph.hammerschmidt@hr.de, www.hr-online.de

ZDF: Christoph Bach, bach.c@zdf.de, www.zdf.de

DJV
Deutscher Journalisten-Verband
Gewerkschaft der Journalistinnen und Journalisten

PRESSEHAUS 2107
SCHIFFBAUERDAMM 40
10117 BERLIN
TEL: 030/72 62 79 20
TELEFAX 030/726 27 92 13

E-MAIL: DJV@DJV.DE
INTERNET: WWW.DJV.DE

Gerichtsentscheidungen mit datenschutzrechtlichem Schwerpunkt 2015

Gerichtshof der Europäischen Union, Urteil vom 6. Oktober 2015 in der Rechtssache C-362/14 Maximilan Schrems ./. Data Protection Commissioner[1]

In dem Verfahren ging es um die Wirksamkeit der sogenannten Safe Harbor-Entscheidung der Europäischen Kommission vom 26. Juli 2000 (2000/520/EG)[2]. Grundlage dieser Entscheidung ist Artikel 25 Absatz 6 der Datenschutzrichtlinie 95/46/EG, wonach die Kommission feststellen kann, dass ein Drittstaat ein angemessenes Schutznivea aufweist und deswegen personenbezogene Daten in dieses Land übermittelt werden dürfen, ohne dass zusätzliche Garantien erforderlich sind. Safe Harbor ist ein in den USA etabliertes, von der US-Handels- und Verbraucherschutzbehörde überwachtes Selbstzertifizierungsmodell, nach dem sich die Unternehmen verpflichten, bestimmte Grundsätze und Prinzipien einzuhalten. In der Entscheidung 2000/520 hatte die Kommission festgestellt, dass ein angemessenes Schutzniveau gewährleistet ist, wenn sich die Organisation, die die Daten erhalten soll, eindeutig und öffentlich verpflichtet, die Grundsätze des „sicheren Hafens" zum Datenschutz einzuhalten, wie sie in den vom US-Handelsministerium am 21. Juli 2000 als „Häufig gestellte Fragen" herausgegebenen Leitlinien umgesetzt wurden.

In seinem Urteil vom 6. Oktober 2015 hat der EuGH zunächst festgestellt, dass alle Unionsbürger die nach Artikel 28 der Richtlinie 95/46 eingerichteten Kontrollstellen anrufen können, wenn sie der Auffassung sind, dass eine Übermittlung ihrer personenbezogenen Daten in ein Drittland unzulässig ist, weil es dort kein angemessenes Datenschutzniveau gibt. Ungeachtet einer Entscheidung der Kommission gemäß Artikel 25 Absatz 6 dieser Richtlinie sind die Aufsichtsbehörden auch verpflichtet, dieser Beschwerde nachzugehen und den zugrundeliegenden Sachverhalt zu prüfen. Allerdings sind sie nicht befugt, eine Entscheidung der Kommission nach Artikel 25 Absatz 6 für ungültig zu erklären. Dies obliege allein dem Europäischen Gerichtshof, um sicherzustellen, dass Unionsrecht einheitlich ausgelegt und angewandt wird.

Bei seiner Überprüfung des Unionsrechts kommt sodann der EuGH zu dem Ergebnis, dass die Entscheidung der Kommission 2000/520 ungültig ist.

Bei der Überprüfung, ob es im Drittland, in das personenbezogene Daten übertragen werden sollen, ein angemessenes Datenschutzniveau gibt, sei darauf abzustellen, ob es dort ein Schutzniveau der Freiheiten und Grundrechte gibt, das dem in der Europäischen Union aufgrund der Richtlinie 95/46/EG im Licht der Charta der Grundrechte garantierten Niveau der Sache nach gleichwertig ist. Dieses Schutzniveau müsse die Rechtsordnung des Drittlandes gewährleisten.

Dabei müsse wegen des Umstandes, dass das in einem Drittland gewährleistete Schutzniveau Veränderungen unterworfen sei, im Anschluss an eine Entscheidung nach Artikel 25 Absatz 6 in regelmäßigen Abständen überprüft werden, ob die Feststellungen zur Angemessenheit des Schutzniveaus in sachlicher und rechtlicher Hinsicht unverändert aufrecht zu erhalten seien.

In seiner rechtlichen Bewertung weist der Gerichtshof darauf hin, dass nach der Safe Harbor-Entscheidung der Kommission die Regelungen des US-amerikanischen Rechts vorgehen und eine

---

[1] Abrufbar unter: http://eur-lex.europa.eu/legalcontent/DE/TXT/HTML/?uri=CELEX:62014CJ0362/from=DE

[2] Abrufbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32000D0520&from=de

weite Ausnahme für Zugriffe, etwa zu Zwecken der nationalen Sicherheit vorgesehen sind. Deswegen hätte die Kommission prüfen müssen, ob das US-amerikanische Recht und die Praxis aufgrund ihrer innerstaatlichen Rechtsvorschriften und internationalen Verpflichtungen einen dem europäischen Niveau „der Sache nach gleichwertigen" Schutz von Freiheiten und Grundrechten bietet. Die Kommission hätte analysieren und positiv feststellen müssen, welche Grenzen das US-amerikanische Recht den Zugriffsbefugnissen von Behörden auf personenbezogene Daten setzt und ob es für die Betroffenen wirksame Rechtsschutzmöglichkeiten gibt.

Der EuGH nimmt in diesem Zusammenhang Bezug auf Mitteilungen der Kommission aus dem Jahr 2013 zu den weitreichenden Zugriffsbefugnissen US-amerikanischer Behörden auf personenbezogene Daten und den fehlenden Rechtsschutzmöglichkeiten von Unionsbürgern. Er stellt fest, dass eine Regelung, die Behörden einen generellen Zugriff auf den Inhalt der elektronischen Kommunikation gestattet, den Wesensgehalt des durch Artikel 7 der Charta der Grundrechte der Europäischen Union garantierten Grundrechts auf Achtung des Privatlebens verletze. Desgleichen verletze eine Regelung, die keine Rechtsbehelfe für Bürger vorsehe, den Wesensgehalt von Artikel 47 der Charta der Grundrechte der Europäischen Union.

Bundesarbeitsgericht, Urteil vom 19. Februar 2015 – 8 AZR 1007/13

In dem vom Bundesarbeitsgericht entschiedenen Fall ging es um die Verwendung von Videoaufnahmen, die ein vom Arbeitgeber beauftragter Detektiv heimlich gefertigt hatte.

Die Klägerin im Ausgangsverfahren war als Sekretärin der Geschäftsleitung tätig. Ab Ende Dezember 2011 war sie arbeitsunfähig erkrankt. Für die Zeit bis zum 28. Februar 2012 legte sie nacheinander vier Arbeitsunfähigkeitsbescheinigungen eines Facharztes für Allgemeinmedizin und danach ab dem 31. Januar 2012 zwei Arbeitsunfähigkeitsbescheinigungen einer Fachärztin für Orthopädie vor. Der Arbeitgeber bezweifelte den als Grund für die letzte Erkrankung mitgeteilten Bandscheibenvorfall und beauftragte einen Detektiv mit der Observation der Klägerin. Diese erfolgte an insgesamt vier Tagen in der Zeit von Mitte bis Ende Februar 2012.

Beobachtet wurden unter anderem das Haus der Klägerin, sie und ihr Mann vor dem Haus und der Besuch der Klägerin in einem Waschsalon. Dabei wurden Videoaufnahmen gefertigt. Der dem Arbeitgeber ausgehändigte Bericht enthielt insgesamt elf Bilder aus diesen Videoaufnahmen. Die Klägerin hält die Anfertigung der Videoaufnahmen für rechtswidrig und fordert ein Schmerzensgeld.

Das Landesarbeitsgericht hielt die Klage für begründet und sprach der Klägerin ein Schmerzensgeld in Höhe von 1.000 EUR zu. Die Revision gegen das Urteil blieb erfolglos. Das Bundesarbeitsgericht stellte fest, dass die Observation einschließlich der gefertigten Videoaufnahmen rechtswidrig war, weil als keinen berechtigten Anlass zu der Überwachung gab. Der Beweiswert der Arbeitsunfähigkeitsbescheinigungen war weder dadurch erschüttert, dass sie von unterschiedlichen Ärzten ausgestellt wurden, noch durch die Änderung im Krankheitsbild oder weil der Bandscheibenvorfall zunächst hausärztlich und erst später fachärztlich behandelt worden war.

Norddeutscher Rundfunk
Rothenbaumchaussee 132
20149 Hamburg
Telefon (040) 41 56-0
E-Mail info@ndr.de
www.ndr.de

Norddeutscher Rundfunk | 20140 Hamburg

Staatsministerium Baden-Württemberg
Referat 35 - Rundfunkpolitik und Medien
Herrn StM Dr. Wolfgang Kreißig
Richard-Wagner-Straße 15
70184 Stuttgart

Ihr Zeichen	Unser Zeichen	Durchwahl	Fax	E-Mail ...@ndr.de	Datum
	Bd/-	-2232	-3697	datenschutz	30.01.2015

Evaluation der Datenschutzbestimmungen im Rundfunkbeitragsstaatsvertrag (RBStV)

Sehr geehrte Damen und Herren,
sehr geehrter Herr Dr. Kreißig,

ich darf mich zunächst ganz herzlich dafür bedanken, dass dem Arbeitskreis der Rundfunk-Datenschutzbeauftragten (AK DSB) Gelegenheit gegeben wird, sich im Rahmen der Evaluierung der Datenschutzbestimmungen im Rundfunkbeitragsstaatsvertrag (RBStV) zu äußern. Der erste Teil dieser Stellungnahme soll den Erfahrungen im Umgang mit den neuen Regelungen und der zweite Teil daraus resultierenden Überlegungen im Kreis der Rundfunk-Datenschutzbeauftragten gewidmet sein. In diesem Zusammenhang möchte ich daran erinnern, dass die Aufsicht über die Einhaltung der Datenschutzbestimmungen beim Einzug des Rundfunkbeitrags von den Rundfunk-Datenschutzbeauftragten wahrgenommen wird und diese insoweit auch die zuständige Stelle für Auskunftsersuchen und Beschwerden von Bürgerinnen und Bürgern sind, die ihre Rechte verletzt sehen. Lediglich bei Radio Bremen, beim Rundfunk Berlin-Brandenburg und beim Hessischen Rundfunk obliegt die Kontrolle der Einhaltung des Datenschutzes beim Rundfunkbeitragseinzug den Landesbeauftragten für Datenschutz (und Informationsfreiheit). Aber auch in diesen drei Rundfunkanstalten sind die Rundfunk-Datenschutzbeauftragten als sogenannte behördliche Datenschutzbeauftragte mit den Auskunftsersuchen und Beschwerden der Bürgerinnen und Bürger im Bereich Rundfunkteilnehmer-Datenverarbeitung befasst.

Erster Teil: Erfahrungsbericht insbesondere zum einmaligen Meldedatenabgleich

Aus datenschutzrechtlicher Sicht ist insbesondere die Umstellung im Privatbereich von der gerätebezogenen Rundfunkgebühr auf den wohnungsbezogenen Rundfunkbeitrag sehr zu begrüßen. Mit dem Inkrafttreten des Rundfunkbeitragsstaatsvertrages (RBStV) ist die Erforschung von Lebenssachverhalten in Familien und Wohngemeinschaften, wie viele Geräte in einer Wohnung vorhanden sind und von wem sie jeweils zum Empfang bereitgehalten werden, obsolet geworden. Gleiches gilt

– außerhalb der Befreiungstatbestände – für die Familien- und Verwandschaftsverhältnisse. Besonders zu begrüßen ist die Entscheidung der Rundfunkanstalten, zukünftig auf den Einsatz eines Beauftragtendienstes zur Feststellung von Sachverhalten im Privatbereich zu verzichten.

Als neues Instrumentarium zur Erfassung von beitragspflichtigen Teilnehmern wurde unter anderem ein einmaliger Meldedatenabgleich durchgeführt. Er erforderte datenschutzrechtlich begründete Einschränkungen und Auflagen, die nach intensiven Diskussionen in entsprechenden Regelungen im RBStV sowie in den Satzungen der Landesrundfunkanstalten ihren Niederschlag gefunden haben.

Diesen umfangreichen Vorgaben ist es wohl zu verdanken, dass der mit großen Datenmengen und dem damit einhergehenden technischen, logistischen und organisatorischen Aufwand verbundene Datenabgleich ohne Datenschutzverstöße abgelaufen ist und nur eine sehr überschaubare Anzahl von Auskunftsersuchen und Beschwerden hervorgerufen hat.

Im Zusammenhang mit den am 1. Januar 2013 in Kraft getretenen Regelungen des Rundfunkbeitragsstaatsvertrages sind bei den Rundfunk-Datenschutzbeauftragten bis heute insgesamt lediglich 463 Auskunftsersuchen und Beschwerden eingegangen, mit denen Bürgerinnen und Bürger die Verletzung von Datenschutzbestimmungen geltend gemacht haben; in dieser Zahl enthalten sind insgesamt 422 Eingaben, die beim Zentralen Beitragsservice in Köln eingegangen sind und sich erkennbar auf den Abgleich mit Meldedaten (anlassbezogene Übermittlung und einmaliger Meldedatenabgleich) bezogen. In 323 dieser Fälle war eine Direktanmeldung vorausgegangen, weil die Adressaten trotz mehrfacher Schreiben des Zentralen Beitragsservice nicht reagierten. Wie viele Beschwerden bei den Beauftragten für Datenschutz (und Informationsfreiheit) in Berlin, Brandenburg, Bremen und Hessen eingegangen sind, ist uns nicht bekannt. In allen übrigen Ländern besteht eine Absprache mit den jeweiligen Landesbeauftragten für Datenschutz (und Informationsfreiheit), dass dort eingehende Beschwerden, die den Datenschutz im Rundfunk einschließlich Beitragseinzug betreffen, zuständigkeitshalber an die jeweilige Rundfunk-Datenschutzbeauftragte oder den jeweiligen Rundfunk-Datenschutzbeauftragten abgegeben werden, so dass sie in den oben aufgeführten Zahlen enthalten sind.

Die ganz überwiegende Anzahl der Eingaben betrafen den einmaligen Meldedatenabgleich, wobei im Regelfall die Erläuterung der Rechtsgrundlage im RBStV sowie der Hinweis auf die damit verbundene Absicht, eine höhere Gerechtigkeit beim Einzug des Rundfunkbeitrags zu erreichen, zu einer Erledigung geführt hat. Deswegen werden sie trotz anderer Bezeichnung im Ergebnis eher als Auskunftsersuchen und weniger als Beschwerden bewertet.

Die Hauptkritik in der Bevölkerung richtete sich erkennbar nicht gegen die Datenschutzbestimmungen im RBStV, sondern gegen dessen Grundlagen und Struktur, mit denen sich inzwischen unter anderem der Verfassungsgerichtshof Rheinland-Pfalz in seiner Entscheidung vom 13. Mai 2014 und der Bayerische Verfassungsgerichtshof in seinen Entscheidungen vom 15. Mai 2014 be-

schäftigt und die Verfassungsmäßigkeit der Regelungen festgestellt hat. Der Bayerische Verfassungsgerichtshof hat sich in seinen Entscheidungen auch ausführlich mit den Anzeige- und Nachweispflichten in § 8 in Verbindung mit § 9 Absatz 2 Satz 1 Nrn. 1 und 3 RBStV und mit dem einmaligen Meldedatenabgleich nach § 14 Absatz 9 RBStV auseinander gesetzt und auch diese Regelungen für mit der Bayerischen Verfassung vereinbar erklärt.

Zweiter Teil: Besteht Änderungs- und Ergänzungsbedarf?

Wiederholter vollständiger Meldedatenabgleich:

Der durchgeführte **Abgleich der Meldedaten** mit dem Teilnehmer-Datenbestand der Rundfunkanstalten hat erkennbar das damit verbundene Ziel erfüllt, zur Vermeidung eines Vollzugsdefizits und zur Herstellung größerer Beitragsgerechtigkeit möglichst alle potentiellen Teilnehmer zu erfassen. Allerdings kann zum gegenwärtigen Zeitpunkt noch nicht abschließend bewertet werden, ob sich hinter den sogenannten Nicht-Reagierern eine nennenswerte Anzahl von tatsächlichen Beitragsschuldnern oder nicht beitragspflichtigen Mitbewohnern verbergen.

Die Landesrundfunkanstalten haben in der Besprechung zur Datenschutzkonformität des RBStV am 21. Oktober 2014 in Berlin vorgetragen, dass allein die staatsvertraglichen Anzeigepflichten und Auskunftsrechte nicht ausreichen, um einer erneuten Erosion des Teilnehmerbestandes wirksam vorzubeugen. Dazu könnte ein – zunächst einmalig – wiederholter vollständiger Meldedatenabgleich dienen.

Nach unseren Erfahrungen ist eine Verschlechterung des Datenbestandes insbesondere in den Fällen zu erwarten, in denen die bisherige Beitragszahlerin oder der bisherige Beitragszahler verstirbt oder umzieht. Trotz der gesetzlichen Anzeigepflicht der in der Wohnung verbleibenden (Gesamt-) Schuldnerin bzw. des in der Wohnung verbleibenden (Gesamt-) Schuldners erhalten in vielen Fällen die Rundfunkanstalten bzw. der Zentrale Beitragsservice keine Information darüber, wer für die entsprechende Wohnung als (neue/neuer) Beitragspflichtige(r) angeschrieben werden kann.

Auch das „Hineinwachsen" Jugendlicher in die Beitragspflicht bleibt vielfach vollständig unentdeckt.

Die zu erwartende Erosion des Datenbestandes lässt sich anhand statistischer Größen ohne weiteres nachvollziehen:

- Etwa 400.000 Menschen versterben jährlich (Durchschnitt der letzten fünf Jahre);
- pro Jahr finden ca. 800.000 Umzüge aufgrund von Scheidungen (ca. 170.000 pro Jahr) oder Trennungen aus anderen Gründen statt;
- ca. 80.000 Personen zogen im Durchschnitt der letzten fünf Jahre ins Ausland um;

- eine unbekannte Anzahl Jugendlicher wohnt schon in einer „eigenen" Wohnung, wenn sie das 18. Lebensjahr vollenden.

Angesichts dieser Daten und der Erfahrung der Landesrundfunkanstalten mit fortschreitender Erosion des Teilnehmerbestands in der Vergangenheit trotz Meldepflichten, Auskunftsrechten und den ergänzend eingesetzten Instrumenten, wie der Anmietung von Adressen bei kommerziellen Adresshändlern oder dem Einsatz von Gebührenbeauftragten, ist es für den AK DSB nachvollziehbar, dass allein der einmalige Meldedatenabgleich nicht ausreichend erscheint, um die dadurch gewonnene hohe Qualität der Daten über die vorhandenen Wohnungsinhaber dauerhaft sichern zu können.

Aus Sicht des AK DSB ist eine – regelmäßige – Wiederholung des vollständigen Meldedatenabgleichs dann möglich und sinnvoll, wenn kein mindestens ebenso geeignetes milderes zur Erreichung der Ziele Vollständigkeit und Richtigkeit des Datenbestandes, Vermeidung eines Vollzugsdefizits und Herstellung von Beitragsgerechtigkeit zur Verfügung steht.

Die Qualität der Meldedaten ist sehr hoch. Soweit – EDV-gestützt – die Zuordnung der Meldedaten zu einer Wohnung, für die Rundfunkbeiträge gezahlt werden, möglich ist, sind die Auswirkungen auf die Betroffenen gering, weil die übermittelten Daten nach kurzer Zeit beim Zentralen Beitragsservice gelöscht werden. In den übrigen Fällen werden die im Zuge der Sachverhaltsklärung ermittelten Beitragsschuldner in den Datenbestand des Beitragsservice übernommen. Wie oben im ersten Teil bereits ausgeführt, ist es bei der Behandlung und Verarbeitung des großen Datenbestandes durch den Zentralen Beitragsservice bei der Durchführung des „einmaligen" Meldedatenabgleichs zu keinen datenschutzrechtlichen Verstößen gekommen. In diesem Zusammenhang ist ergänzend darauf hinzuweisen, dass dieser Prozess auch von der/dem zuständigen Rundfunk-Datenschutzbeauftragten überwacht wurde.

Daten über diejenigen Personen, die im Zuge der Sachverhaltsklärung „ausgesondert" wurden, werden allerdings nicht gespeichert. Es ist zu vermuten, dass sie bei einem erneuten Datenabgleich wiederum zum Zweck der Sachverhaltsklärung angeschrieben werden. Damit ist eine gewisse Belästigung verbunden, die allerdings als gering einzustufen ist.

Diese Einschätzung steht im Einklang mit den vorliegenden landesverfassungsgerichtlichen Entscheidungen. Auch die Landesverfassungsgerichte sehen kein gleich geeignetes, milderes Mittel als den Meldedatenabgleich zum Erhalt des Bestandes und der Qualität der Teilnehmerdaten.[1]

[1] Entscheidung des Bayerischen Verfassungsgerichtshofes vom 15. Mai 2014, Rdnr. 156:
„§ 14 Absatz 9 RBStV greift in dieses Recht ein, indem er anordnet, dass jede Meldebehörde einmalig zum Zwecke der Bestands- und Ersterfassung für einen bundesweit einheitlichen Stichtag automatisiert in standardisierter Form die in Satz 1 im Einzelnen bezeichneten Daten aller volljährigen Personen an die jeweils zuständige Landesrundfunkanstalt übermittelt. Dieser Eingriff ist verfassungsrechtlich gerechtfertigt. Denn die Vorschrift, die dem rechtsstaatlichen Bestimmtheitsgebot ersichtlich genügt, entspricht auch dem Grundsatz der Verhältnismäßigkeit. (...) Die angestrebte Vermeidung eines Vollzugsdefizits und Herstellung

Ein mögliches, in der Vergangenheit genutztes Mittel zur Pflege des Datenbestandes ist die Anmietung von Adressen bei kommerziellen Adresshändlern. Dies ist den Rundfunkanstalten grundsätzlich gestattet, war allerdings durch die Regelung in § 14 Absatz 10 RBStV bis zum 31. Dezember 2014 ausgesetzt. Wie Herr Dr. Eicher in der Sitzung am 21. Oktober 2014 in Berlin berichtete, wird davon zurzeit kein Gebrauch gemacht. Der AK DSB hat wiederholt zum Ausdruck gebracht, dass die Anmietung von Adressen kommerzieller Händler aus datenschutzrechtlicher Sicht nicht zu befürworten ist. Die Qualität der Daten entspricht selbst bei seriösen Anbietern nicht annähernd der Qualität der Meldedaten. Im Unterschied zum Datenbestand der Meldebehörden ist auch nicht die Vollständigkeit des Datenbestandes gesichert, so dass das angemietete Datenmaterial insgesamt weniger geeignet erscheint, um die oben beschriebenen Ziele zu erreichen.

Gleiches gilt für den – inzwischen von den Landesrundfunkanstalten eingestellten – Einsatz von Beauftragten zur Sachverhaltsfeststellung vor Ort. Damit sind nicht unerhebliche Beeinträchtigungen Betroffener verbunden, weil die tatsächlichen Verhältnisse vor Ort überprüft werden und – entgegen der Absicht des Gesetzgebers – „hinter die Wohnungstür" geschaut werden müsste, um festzustellen, welche Personen als Inhaber der Wohnung als Beitragszahler in Betracht kommen.

Weitere ebenfalls geeignete Instrumente zur Vermeidung einer Erosion des Datenbestandes sind nicht ersichtlich.

Fazit: Im Vergleich zu den aufgeführten alternativen Instrumentarien erscheint ein vollständiger Meldedatenabgleich nach unserer Prüfung als das mildeste und am besten geeignete sowie gleichzeitig mit geringen Eingriffen in geschützte Rechtspositionen verbundene Mittel, um einer Erosion des Teilnehmer-Datenbestandes, die (erneut) zu einem Vollzugsdefizit und einer damit verbundenen ungleichen wirtschaftlichen Belastung der Beitragsschuldner führen würde, vorzubeugen. Aus Sicht der Rundfunk-Datenschutzbeauftragten bestehen keine grundsätzlichen Bedenken gegen die Einführung eines wiederholten vollständigen Meldedatenabgleichs im Abstand von fünf bis sechs Jahren, sofern dabei die zu dem 2013/2014 durchgeführten Meldedatenabgleich getroffenen Festlegungen im Staatsvertrag und in den Satzungen (Stichtag, Nutzungsdauer, Löschfristen usw.) auch für alle weiteren Vorhaben dieser Art gelten.

---

größerer Beitragsgerechtigkeit sind legitime Zwecke, die einen Eingriff in das Recht der informationellen Selbstbestimmung rechtfertigen können. (...) Der Gesetzgeber durfte die Vorschrift für erforderlich halten. Auch wenn der einmalige Meldedatenabgleich alle volljährigen Personen betrifft und damit einen äußerst großen Kreis an Betroffenen erfasst, sind weniger beeinträchtigende Mittel, die ebenso weitreichende Aufklärung ermöglichen, nicht zu erkennen."

Erhebung und Nutzung von Telefonnummern und E-Mail-Adressen aus öffentlich zugänglichen Quellen im nicht privaten Bereich:

Der AK DSB regt an, im **nicht privaten** Bereich eine ausdrückliche Rechtsgrundlage für die Erhebung und Nutzung von allgemein zugänglichen Telefonnummern und E-Mail-Adressen zu schaffen.

Sofern eine vorherige schriftliche Kontaktaufnahme nicht möglich oder erfolglos geblieben ist, dürfte im geschäftlichen Verkehr eine telefonische Kontaktaufnahme oder ein Anschreiben per E-Mail eine sinnvolle und Erfolg versprechende Maßnahme zur Sachverhaltsklärung sein. Sie stellen gegenüber einer Sachverhaltsklärung vor Ort das wesentlich mildere Mittel dar. Die im Geschäftsverkehr benutzten Kontaktdaten dienen gerade dazu, zu den Verwendern in geschäftlichen Kontakt zu treten. Im Unterschied zu Privatpersonen wird die in den Landesdatenschutzgesetzen erlaubte Nutzung von Daten aus allgemein zugänglichen Quellen im Geschäftsverkehr für Zwecke des Geschäftsverkehrs auch nicht durch Regelungen über unzumutbare Belästigungen eingeschränkt (vgl. § 7 UWG). Ein Pilotversuch zur Sachverhaltsklärung im nicht privaten Bereich auf diesem Weg ist erfolgreich verlaufen.

Bei Betriebsstätten von Einzelkaufleuten oder Freiberuflern handelt es sich bei Telefonnummern und E-Mail-Adressen fast immer auch um personenbezogene Daten. Deshalb sollte in § 11 RBStV, wonach eine Erhebung personenbezogener Daten bei öffentlichen und nicht öffentlichen Stellen ohne Kenntnis der Betroffenen erlaubt ist, eine Ergänzung aufgenommen werden, die es den Landesrundfunksanstalten ausdrücklich gestattet, **im nicht privaten Bereich** Telefonnummern und E-Mail-Adressen aus öffentlich zugänglichen Quellen zu nutzen. Dies sollte – im Hinblick auf Einzelkaufleute und Freiberufler – auf solche Daten beschränkt sein, die erkennbar im Geschäftsverkehr verwendet werden.

Kreis der zur Auskunft Verpflichteten nach § 9 Absatz 1 RBStV:

Bei einer Überarbeitung des RBStV sollte in § 9 Absatz 1 der Kreis der zur Auskunft Verpflichteten noch einmal überdacht werden. Dort ist neben dem Eigentümer „der vergleichbar dinglich Berechtigte" aufgeführt. Dieser Begriff erscheint nicht ausreichend bestimmt, weil es dafür weder eine gesetzliche Definition noch einen beispielsweise durch die Rechtsprechung geprägten feststehenden Kreis von Personen gibt. Es bietet sich an, diesen Personenkreis, wer immer damit gemeint sein soll, ersatzlos entfallen zu lassen.

Sperren für die Übermittlung von Daten (§ 11 Absatz 4 RBStV):

In § 11 Absatz 4 letzter Satz RBStV sollte zur Klarstellung ein Hinweis aufgenommen werden, in welchen Fällen Sperren einer Übermittlung an die Rundfunkanstalten bzw. an den von ihnen beauftragten Zentralen Beitragsservice entgegenstehen. Dies ist nur bei den gesetzlich ausdrücklich vorgesehenen Übermittlungssperren, wie insbesondere bei Adoptionspflegeverhältnissen oder bei

Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnlich schutzwürdige Interessen der Fall (vgl. §§ 51, 52 Bundesmeldegesetz, das am 1. November 2015 in Kraft tritt). Andere Sperren, wie beispielsweise für Direktwerbung, für die Übermittlung an Parteien, an öffentlich-rechtliche Religionsgemeinschaften oder an Kreiswehrersatzämter, stehen einer Übermittlung an die Rundfunkanstalten oder den Zentralen Beitragsservice nicht entgegen. Eine solche Klarstellung ist aus Sicht des Datenschutzes zu begrüßen, weil es für die Betroffenen Transparenz und Klarheit schafft, dass nicht jede Auskunftssperre einer Übermittlung an die Rundfunkanstalten bzw. den Zentralen Beitragsservice entgegensteht.

Übernahme von Satzungsbestimmungen in den Staatsvertrag:

§ 7 der Satzung enthält nähere Regelungen über die Datenerhebung bei öffentlichen Stellen. Im Sinn der Normenklarheit wäre es zu begrüßen, wenn diese Regelungen in den RBStV überführt würden.

Mit freundlichen Grüßen

Horst Brendel
Datenschutzbeauftragter

Chronologische Aufstellung von Projekten und Vorhaben zur Verarbeitung personenbezogener Daten im NDR in 2015

Bezeichnung	votiert am:
DV-Projekt: Immobilienverwaltung – Nutzererweiterung	07.01.2015
DV-Projekt: Entwicklung eines zentralen Loggings für Sophora DeskClients	16.01.2015 18.02.2015 20.03.2015
DV-Projekt: Produktion anmelden mit System (PASY)	22.01.2015
DV-Projekt: Pilottest FireEye	26.02.2015
DV-Projekt: Deutscher Web Video Preis	19.03.2015
DV-Projekt: Flypsite für Social TV	03.03.2015
DV-Peojekt: Logging im Sophora DeskClient	20.03.2015
DV-Projekt: Fernsehtechnische Einrichtungen zur Ausstattung von Studio, Fernsehregie u. Betriebsabwicklung Fernsehen im Landesfunkhaus Hannover	25.03.2015
DV-Projekt: Ersatz Betriebsabwicklung Hörfunk	26.03.2015
DV-Projekt: Lizenzmanagementsystem SmartTrack	22.04.2015
DV-Projekt: neues Hörfunkstudio in Neu Delhi	04.05.2015
DV-Projekt: Erneuerung FS-Technik Landesstudios MV	27.05.2015
DV-Projekt: NLE Ersatz Schneideräume Hamburg	04.06.2015
DV-Projekt: Regelbetrieb VPN quick Xchange	24.06.2015
DV-Projekt: Konsolidierung der Telekommunikations-Abrechnungssysteme im NDR	15.07.2015 14.08.2015
DV-Projekt: Zusammenführung Schalträume und Leitungsbüros HH	30.07.2015
DV-Projekt: Erneuerung HF-Produktionsregie 8	14.09.2015
DV-Projekt: E-Recruiting	05.10.2015 06.01.2016
DV-Projekt: Erneuerung FS-Technik Landesstudios Schleswig-Holstein und Niedersachsen	06.10.2015

DV-Projekt Elbphilharmonie Audiotechnik	04.11.2015
DV-Projekt Budgetüberwachung und Budget-Abrechnung für Aushilfen	15.12.2015
DV-Projekt: IT-Projekt 6164/ Revisionssoftware	15.12.2015
DV-Projekt; Pilot Web- und Videokonferenz	28.12.2015

Zusammenfassung der Eingaben und Beschwerden von Rundfunkteilnehmern

Datum Ein-/ Ausgang	Gegenstand der Eingabe	erledigt durch
16.12.14 / 12.01.15	Auskunftsersuchen	DSB NDR mit Unterstützung Abt. Beitragsservice
09.01.15 / 12.01.15	Auskunftsersuchen	DSB NDR mit Unterstützung Abt. Beitragsservice
09.01.15 / 12.01.15	Auskunftsersuchen	DSB NDR mit Unterstützung Abt. Beitragsservice
13.01.15 / 26.01.15	Auskunftsersuchen	DSB NDR mit Unterstützung Abt. Beitragsservice
24.01.15 / 13.02.15	Auskunftsersuchen	DSB NDR mit Unterstützung Abt. Beitragsservice
06.02.15 / 12.02.15	Auskunftsersuchen	Weitergabe an HR
07.02.15 / 09.02.15	Fragen zum Datenschutz bei Beitragsbefreiungsanträgen	DSB NDR
17.03.15 / 18.03.15	Auskunftsersuchen	DSB NDR mit Unterstützung Abt. Beitragsservice
	Ungeklärte Differenzen bei Speicherung d. Beitragsdaten	DSB NDR mit Unterstützung Abt. Beitragsservice
20.07.15 / 24.07.15	Auskunftsersuchen	DSB NDR mit Unterstützung Abt. Beitragsservice
20.08.15 / 21.08.15	Bitte um Weitergabe der Abmeldung	Abgabe an Abt. Beitragsservice
10.08.15 / 25.08.15	Beschwerde über Vollstreckungsauftrag	Abgabe an Abt. Beitragsservice
17.08.15 / 01.09.15	Auskunftsersuchen	DSB NDR mit Unterstützung Abt. Beitragsservice
17./18.08. / 09.09.15 28.09.15	Auskunftsersuchen	DSB NDR mit Unterstützung Abt. Beitragsservice
18.6./18.8. / 21.9.15 ü/Hmb.BfDI	Verwendung falscher Adressdaten	DSB NDR mit Unterstützung Abt. Beitragsservice
15.09. / 05.10.15	Beschwerde zur Betriebsstätten-Anmeldung	DSB NDR mit Unterstützung Abt. Beitragsservice

Zusammenfassung der Eingaben und Beschwerden von Rundfunkteilnehmern

Datum Ein-/ Ausgang	Gegenstand der Eingabe	erledigt durch
07.09. / 05.10.15 ü/Hmb.BfDI	Mailingaktion an Verstorbenen	DSB NDR mit Unterstützung Abt. Beitragsservice
08.10.15 / 02.11.15	Auskunftsersuchen	DSB NDR mit Unterstützung Abt. Beitragsservice
16.11.15 / 19.11.15	Auskunftsersuchen	DSB NDR mit Unterstützung Abt. Beitragsservice
20.11.15 / 24.11.15	Auskunftsersuchen nach BDSG	DSB NDR
30.11.15 / 02.12.15	Fragen zur Einzugsermächtigung	DSB NDR mit Unterstützung ZBS
02.12.15 / 07.12.15	Fragen zur Beitragsbefreiung	DSB NDR
06.12.15 / 09.12.15	E-Mail-Verschlüsselung	DSB NDR
15.12.15 / 05.01.16	Auskunftsersuchen	DSB NDR mit Unterstützung Abt. Beitragsservice
15.12.15 / 07.01.16	Auskunftsersuchen	DSB NDR mit Unterstützung Abt. Beitragsservice

Arbeitskreis der Rundfunkdatenschutzbeauftragten (AK DSB)
Wesentliche Themenschwerpunkte der Sitzungen im Jahr 2015

- Anforderung von Auswertungen zur Nutzung der Sphinx-Datenbanken des ZDF durch Landesrundfunkanstalten
- Anhörung Evaluierung Rundfunkbeitragsstaatsvertrag
- Aufnahme mit verdeckten Kameras: Google Glass
- Aufgabenverteilung zum Datenschutz bei den Partnerkanälen (3sat, Phoenix, Kinderkanal) und Gemeinschaftseinrichtungen
- Datenschutz beim Beihilfeberechnungszentrum bbz
- Datenschutz bei der Baden-Badener Pensionskasse
- Datenschutz bei HbbTV
- Dienstvereinbarung zu SAP?
- Entwicklungen im nationalen Datenschutzrecht: Verbandsklagerecht im Datenschutz
- Einsatz von „Dropbox"? / ARD/ZDF-Box des IVZ
- EU-Datenschutzgrundverordnung
- IT-Sicherheitsgesetz
- Novellierung WDR-Gesetz
- Nutzung und Speicherung von Telefonnummern und E-Mailadressen von Rundfunkteilnehmern durch den ZBS
- Personalisierung öffentlich-rechtlicher Onlineangebote
- Rechtsstreit VZBV ./. MDR wegen der KiKa-Gewinnspielpraxis, Entscheidung des BGH
- Regelmäßiger Datenabgleich und Asylbewerber
- Sicherheitslücken bei SIM-Karten von Telekom und Vodafone
- Stand der Überlegungen zum Minderjährigendatenschutz
- Stellungnahme zur Evaluierung der Datenschutzbestimmungen im Rundfunkbeitrags-staatsvertrag
- Stellungnahme zum Entwurf eines neuen Gesetzes zur Vorratsdatenspeicherung
- Struktur der Aufsichtsbehörden in Deutschland: Informationsaustausch mit Datenschutzbeauftragten der EKD und BLM

Arbeitskreis der Rundfunkdatenschutzbeauftragten (AK DSB)
Wesentliche Themenschwerpunkte der Sitzungen im Jahr 2015

- Überarbeitung des Social Media-Leitfadens
- Umsetzung der Cookie-Richtlinie in Deutschland
- Vergabesoftware
- Vorschlag der deutschen Delegation zum „Recht auf Vergessenwerden"
- Youngdata – das gemeinsame Jugendportal der Datenschutzbeauftragten des Bundes und der Länder

Position, Aufgaben und Befugnisse des Datenschutzbeauftragten des NDR

Der Datenschutzbeauftragte (DSB) des NDR wird aufgrund von **§ 41 des NDR Staatsvertrages (NDR StV)** tätig. Seine Aufgabe besteht gemäß § 41 Abs. 3 NDR StV vor allem in der **Überwachung der Einhaltung der Vorschriften über den Datenschutz** bei der Tätigkeit des NDR. Dies gilt auch für den Fall, dass Dritte im Auftrage des NDR tätig werden (§ 41 Abs. 3 Satz 2 NDR StV), wie beispielsweise der ARD ZDF und Deutschlandradio Beitragsservice in Köln.

Für den Datenschutz des - gesamten - NDR gilt gemäß § 41 Abs. 1 NDR StV neben den Bestimmungen des NDR Staatsvertrages **das Hamburgische Datenschutzgesetz (HmbDSG)** vom 5. Juli 1990, zuletzt geändert durch Gesetz vom 5. April 2013. Dies bedeutet, dass auf das Handeln des NDR auch in den Bundesländern Mecklenburg-Vorpommern, Niedersachsen und Schleswig-Holstein ergänzend zu den datenschutzrechtlichen Regelungen in §§ 41 und 42 NDR StV das Hamburgische Datenschutzgesetz Anwendung findet und nicht die Datenschutzgesetze dieser Bundesländer.

Die Aufgaben des DSB NDR beschreibt § 41 NDR StV im einzelnen dahingehend, dass er

- die Einhaltung der Vorschriften über den Datenschutz überwacht, auch soweit Dritte im Auftrag des NDR tätig werden (§ 41 Abs. 1 S. 1 und 2);
- die Intendantin oder den Intendanten und den Verwaltungsrat in Fragen des Datenschutzes berät (§ 41 Abs. 3 Satz 3 Halbsatz 2);
- Empfehlungen zur Verbesserung des Datenschutzes geben kann (§ 41 Abs. 3 Satz 3 Halbsatz 1).

Um sich die erforderlichen Informationen und Erkenntnisse für seine Tätigkeit verschaffen zu können, stehen dem Datenschutzbeauftragten

- Auskunfts- und Einsichtsbefugnisse in alle Unterlagen und Akten — vor allem in gespeicherte Daten und Datenverarbeitungsprogramme —, die mit der Verarbeitung personenbezogener Daten in Zusammenhang stehen,

sowie

- ein Zutrittsrecht zu allen Diensträumen

zu (§ 41 Abs. 3 Satz 5 Ziffern 1 und 2). In diesem Zusammenhang ist bedeutsam, dass gesetzliche Geheimhaltungsvorschriften einem Auskunfts- oder Einsichtsverlangen des Datenschutzbeauftragten nicht entgegengehalten werden können (§ 41 Abs. 3 Satz 6).

Der Intendant unterstützt den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben (§ 41 Abs. 3 Satz 4).

Für den Fall, dass er Verstöße gegen Datenschutzbestimmungen oder sonstige Mängel bei der Verarbeitung personenbezogener Daten feststellt,

- beanstandet der Datenschutzbeauftragte die von ihm festgestellten Verstöße oder Mängel gegenüber dem Intendanten und fordert eine Stellungnahme binnen einer von ihm zu bestimmenden Frist an (§ 41 Abs. 5 Satz 1). Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandung getroffen worden sind (§ 41 Abs. 5 Satz 2).
- Soweit binnen der vom Datenschutzbeauftragten gesetzten Frist ein Verstoß oder ein sonstiger Mangel nicht behoben worden sind, richtet der Datenschutzbeauftragte eine weiterführende Beanstandung an den Verwaltungsrat (§ 41 Abs. 5 Satz 3).

- Der Datenschutzbeauftragte kann von einer Beanstandung absehen oder auf eine Stellungnahme verzichten, wenn es sich um Fälle von geringer Bedeutung handelt oder wenn die Behebung der Mängel sichergestellt ist (§ 41 Abs. 6).

Mit der Beanstandung kann der Datenschutzbeauftragte Vorschläge zur Mängelbeseitigung oder Anregungen zur sonstigen Verbesserung des Datenschutzes verbinden (§ 41 Abs. 7).

Jede Bürgerin und jeder Bürger kann sich an den Datenschutzbeauftragten wenden, wenn sie oder er der Ansicht ist, durch den NDR oder durch einen im Auftrag des NDR tätig werdenden Dritten bei der Verarbeitung ihrer oder seiner Daten in ihren oder seinen schutzwürdigen Interessen verletzt zu sein (§ 41 Abs. 8).

Nach § 41 Abs. 9 erstattet der Datenschutzbeauftragte dem Verwaltungsrat jährlich einen Tätigkeitsbericht.

Verfahrenskodex der Rundfunkbeauftragten für den Datenschutz zur Behandlung von Eingaben oder Hinweisen Dritter

(1) Die Rundfunkbeauftragten für den Datenschutz [RfD] sind bestrebt, **Eingaben oder Hinweise Dritter möglichst zeitnah und effizient zu bearbeiten**. Damit soll zum einen eventuellen Missständen abgeholfen werden, aber es sollen auch im jeweiligen Verantwortungsbereich der RfD geeignete Maßnahmen getroffen werden können, die datenschutzrechtliche Standards ergänzen oder verbessern.

(2) Die RfD unterstützen den Bürger bei der **konkreten Wahrung seines individuellen Rechts auf informationelle Selbstbestimmung im Bereich des Rundfunkwesens**; dementsprechend werden Auskünfte zu allgemeinen datenschutzrechtlichen Fragen nachrangig und - soweit möglich - formalisiert erteilt.

(3) Die RfD nehmen **Eingaben oder Hinweise vorzugsweise in schriftlicher Form** (Brief, Telefax, eMail, evtl. SMS) entgegen. Dadurch werden Missverständnisse vermieden und die Legitimation des Petenten leichter nachvollziehbar gemacht.

Werden Eingaben oder Hinweise einem RfD mündlich vorgetragen, wird er aus den dargelegten Gründen regelmäßig darum bitten, schriftlich über das konkrete Anliegen informiert zu werden.

(4) In Fällen besonderer Dringlichkeit oder der Verhinderung des Petenten an einem schriftlichen Vortrag oder bei unkomplizierten, kurzfristig zu klärenden Sachverhalten erledigt der RfD den Vorgang ggf. auch aufgrund (fern-)mündlicher Anfrage.

(5) Bei der Entgegennahme von Eingaben oder Hinweisen prüft der RfD, u.a. um seine eigene territoriale Zuständigkeit sicherzustellen, die **Identität des Petenten**; dabei ist mindestens der genaue Name und die Wohnanschrift festzustellen; bei Eingaben, die das Rundfunkgebührenwesen betreffen, verschafft sich der RfD ggf. auch Kenntnis über die Teilnehmernummer. Bei Zweifeln an der Geschäftsfähigkeit – so u.a. evtl. an der Volljährigkeit – eines Petenten stellt der RfD erforderliche Informationen sicher.

Soweit der Petent nicht bereit ist, sich zu identifizieren, oder erkennbar ungenaue Angaben macht, ist der RfD nicht verpflichtet, sich auf andere Weise Gewissheit über die Identität des Petenten zu verschaffen.

Bei fehlenden Anhaltspunkten oder Zweifeln an der Identität eines Petenten ist der RfD berechtigt, eine Behandlung oder Bearbeitung der Eingabe oder des gegebenen Hinweises zu verweigern.

(6) Eine Eingabe oder ein Hinweis hat mindestens so bestimmt zu sein, dass der aufgegriffene **Sachverhalt und das konkrete Anliegen verständlich** sind. Mangelt es im Einzelfall lediglich an bestimmten Detailangaben, stellt der RfD durch gezielte Nachfrage beim Petenten die vollständige Aufklärung des Sachverhaltes oder Anliegens sicher.

Ist weder eine Sachverhalts- noch eine Anliegensklärung möglich, beendet der RfD die Behandlung der Angelegenheit.

(7) Der RfD behandelt regelmäßig **keine Eingaben oder Hinweise beleidigenden Inhalts** oder in herabwürdigender Form vorgetragene Anliegen.

(8) Der RfD wickelt seine Korrespondenz aus Gründen der Vertraulichkeit und Datensicherheit **grundsätzlich nur auf dem Briefweg** ab. Andere Kommunikationswege (Telefax, eMail oder SMS) werden durch den RfD nur verwendet, wenn sie zuvor mit dem Petenten abgestimmt

wurden oder der Petent sich seinerseits durch Form und Darstellung in seiner Eingabe mit einer Abwicklung auf einem anderen Kommunikationswege einverstanden gezeigt hat.

(9) Ist der RfD aufgrund der für ihn erkennbaren Umstände nach eigener Einschätzung nicht in der Lage, zu einer Eingabe oder einem Hinweis kurzfristig (i.e. regelmäßig binnen eines Monats nach Erhalt) abschließend Stellung zu nehmen, erteilt er dem Petenten einen **Zwischenbescheid**.

(10) Wird die Angelegenheit **von dritter Seite an den RfD abgegeben**, bestätigt der RfD dem Übermittelnden die Übernahme der Angelegenheit dann, wenn dies nicht bereits durch die abgebende Stelle geschehen ist oder die abschließende Beantwortung der Eingabe nicht zeitnah erfolgen kann.

(11) Bei sich langfristig hinziehenden Angelegenheiten lässt der RfD einem Petenten in regelmäßigen Abständen – ca. alle drei Monate – unaufgefordert eine **Zwischennachricht** zukommen.

(12) Der RfD stellt bei Vornahme seiner Recherchen und den ggf. anschließend von ihm ergriffenen oder eingeleiteten Maßnahmen die **nötige Vertraulichkeit** sicher, die verhindert, dass dem Petenten wegen seiner Kontaktaufnahme mit dem RfD irgendwelche Nachteile erwachsen.

(13) Der RfD erteilt dem Petenten nach **Abschluss der Bearbeitung eine Nachricht**, in der in angemessener Form und gebotenem Umfang über die getroffenen Feststellungen und ergriffenen Maßnahmen berichtet wird. Der RfD erhebt für seine Tätigkeit keine Gebühren oder Entgelte vom Petenten.

Rückfragen des Petenten zu der ihm abschließend erteilten Nachricht behandelt der RfD, soweit dem Anliegen des Petenten damit noch zusätzlich Rechnung getragen werden kann.

(14) Der RfD berichtet über Angelegenheiten von besonderer Bedeutung oder außerordentlicher Tragweite in anonymisierter Form in seinem **Tätigkeitsbericht**.

14. Oktober 2005 / 21. September 2006

Arbeitskreis der Rundfunkbeauftragten
für den Datenschutz

Artikel 28 –EG-Datenschutzrichtlinie - Kontrollstelle

(1) Die Mitgliedstaaten sehen vor, dass eine oder mehrere öffentliche Stellen beauftragt werden, die Anwendung der von den Mitgliedstaaten zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in ihrem Hoheitsgebiet zu überwachen. Diese Stellen nehmen die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahr.

(2) Die Mitgliedstaaten sehen vor, dass die Kontrollstellen bei der Ausarbeitung von Rechtsverordnungen oder Verwaltungsvorschriften bezüglich des Schutzes der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten angehört werden.

(3) Jede Kontrollstelle verfügt insbesondere über:

- Untersuchungsbefugnisse, wie das Recht auf Zugang zu Daten, die Gegenstand von Verarbeitungen sind, und das Recht auf Einholung aller für die Erfüllung ihres Kontrollauftrags erforderlichen Informationen;
- wirksame Einwirkungsbefugnisse, wie beispielsweise die Möglichkeit, im Einklang mit Artikel 20 vor der Durchführung der Verarbeitungen Stellungnahmen abzugeben und für eine geeignete Veröffentlichung der Stellungnahmen zu sorgen, oder die Befugnis, die Sperrung, Löschung oder Vernichtung von Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung anzuordnen, oder die Befugnis, eine Verwarnung oder eine Ermahnung an den für die Verarbeitung Verantwortlichen zu richten oder die Parlamente oder andere politische Institutionen zu befassen;
- das Klagerecht oder eine Anzeigebefugnis bei Verstößen gegen die einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie. Gegen beschwerende Entscheidungen der Kontrollstelle steht der Rechtsweg offen.

(4) Jede Person oder ein sie vertretender Verband kann sich zum Schutz der die Person betreffenden Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten an jede Kontrollstelle mit einer Eingabe wenden. Die betroffene Person ist darüber zu informieren, wie mit der Eingabe verfahren wurde.

Jede Kontrollstelle kann insbesondere von jeder Person mit dem Antrag befasst werden, die Rechtmäßigkeit einer Verarbeitung zu überprüfen, wenn einzelstaatliche Vorschriften gemäß Artikel 13 Anwendung finden. Die Person ist unter allen Umständen darüber zu unterrichten, dass eine Überprüfung stattgefunden hat.

(5) Jede Kontrollstelle legt regelmäßig einen Bericht über ihre Tätigkeit vor. Dieser Bericht wird veröffentlicht.

(6) Jede Kontrollstelle ist im Hoheitsgebiet ihres Mitgliedstaats für die Ausübung der ihr gemäß Absatz 3 übertragenen Befugnisse zuständig, unabhängig vom einzelstaatlichen Recht, das auf die jeweilige Verarbeitung anwendbar ist. Jede Kontrollstelle kann von einer Kontrollstelle eines anderen Mitgliedstaats um die Ausübung ihrer Befugnisse ersucht werden.

Die Kontrollstellen sorgen für die zur Erfüllung ihrer Kontrollaufgaben notwendige gegenseitige Zusammenarbeit, insbesondere durch den Austausch sachdienlicher Informationen.

(7) Die Mitgliedstaaten sehen vor, dass die Mitglieder und Bediensteten der Kontrollstellen hinsichtlich der vertraulichen Informationen, zu denen sie Zugang haben, dem Berufsgeheimnis, auch nach Ausscheiden aus dem Dienst, unterliegen.