Bayerische Landeszentrale für neue Medien

Dreizehnter Tätigkeitsbericht
des Beauftragten für den Datenschutz
bei der Bayerischen Landeszentrale für neue Medien

(Berichtszeitraum: 01.01.2016 bis 31.12.2017; im Hinblick auf die am 25.05.2018 eingetretene Rechtsänderung enthält der Bericht auch Ausführungen zum Zeitraum vom 01.01.2018 bis 25.05.2018)

An den

Vorsitzenden des Medienrats
Herrn Walter Keilbart

Vorsitzenden des Verwaltungsrats
Herrn Manfred Nüssel

Präsidenten der
Bayerischen Landeszentrale
für neue Medien
Herrn Siegfried Schneider
im Hause

Unser Zeichen: 3./6.11 · Telefon: 089 63808-161 · Fax: -185 · 24.05.2019
Ihr Schreiben vom · Ihr Zeichen:

Dreizehnter Tätigkeitsbericht des Beauftragten für den Datenschutz
bei der Bayerischen Landeszentrale für neue Medien

Sehr geehrter Herr Keilbart,
sehr geehrter Herr Nüssel,
sehr geehrter Herr Schneider,

in der Anlage übersende ich Ihnen gemäß Art. 20 Abs. 6 S. 2 des Bayerischen Mediengesetzes in der bis einschließlich 24.05.2018 geltenden Fassung den dreizehnten Tätigkeitsbericht des Beauftragten für den Datenschutz bei der Bayerischen Landeszentrale für neue Medien.

Mit freundlichen Grüßen

Andreas Gummer
Beauftragter für den Datenschutz

Inhalt

1 Vorbemerkung

Gem. Art. 20 Abs. 6 S. 2 BayMG in der bis einschließlich 24.05.2018 geltenden Fassung erstattet der Beauftragte für den Datenschutz den Organen der Landeszentrale mindestens alle zwei Jahre einen Bericht über seine Tätigkeit.

Der vorliegende Bericht ist der dreizehnte Tätigkeitsbericht seit Inkrafttreten des BayMG am 01.12.1992 und bezieht sich auf die Jahre 2016 und 2017.[1] Im Hinblick auf die mit der DS-GVO, welche ab dem 25.05.2018 in allen Mitgliedstaaten der EU verbindlich anzuwenden ist, eintretenden weitreichenden Veränderungen in den normativen Vorgaben wurde der vorliegende Bericht um Ausführungen für den Zeitraum vom 01.01.2018 bis zum 25.05.2018 ergänzt.
Der Schwerpunkt meiner Tätigkeit lag im Berichtzeitraum neben der Beratung von Landeszentrale und Anbietern im Hinblick auf die Anforderungen des Datenschutzrechts und der sich für den betrieblichen Ablauf daraus ergebenden Folgerungen vor allem auch in der anlassbezogenen Kontrolle der Einhaltung und Umsetzung datenschutzrechtlicher Vorgaben aufgrund wie auch unabhängig von eingehenden Beschwerden.
Einen maßgeblichen Bestandteil der Arbeit bildete weiterhin der Umgang mit den im Berichtszeitraum aufgetretenen Datenpannen. Daneben erlangte auch der Themenkomplex „unerwünschte Werbung" eine besondere Bedeutung. Weiterhin virulent war die Frage, welche Sicherheitsanforderungen sich aus Datenschutzvorgaben ergeben, und wie hierauf im täglichen Umgang (vor allem auch bei der Konzeptionierung von IT-Systemen) zu reagieren ist. Insgesamt kann festgestellt werden, dass die Nutzer in Fragen des Datenschutzes unterdessen sensibilisierter sind, kritischer reagieren und verstärkt ihre Rechte wahrnehmen.

Förmliche Beanstandungen musste ich im Berichtzeitraum nicht aussprechen, wenn auch die Rahmenbedingungen sich in diesem Zusammenhang deutlich verschoben haben.

[1] Zitierte Normen beziehen sich auf die jeweilige damalige Fassung im Berichtszeitraum

2 Entwicklung des Datenschutzrechts

2.1 Internationale Entwicklungen

Aufgrund der stetig wachsenden Internationalisierung der Weltwirtschaft nimmt der weltweite Datenaustausch stetig zu und gewinnt an Bedeutung, so dass es unterdessen unerlässlich geworden ist, diese Entwicklungen zu beachten und daher auch über sie zu berichten.

2.1.1 Urteil des EuGH vom 06.10.2015 zum Safe Harbour-Abkommen

Wie bereits im letzten Tätigkeitsbericht erwähnt,[2] hat der EuGH mit Urteil vom 06.10.2015 festgestellt, dass das Safe Harbour-Abkommen[3] zwischen den USA und der EU ungültig ist.[4]

Der Entscheidung des EuGH lag ein Rechtsstreit des österreichischen Staatsbürgers Max Schrems mit der irischen Datenschutzbehörde zugrunde, die wegen des Sitzes der Europazentrale von Facebook in Irland zuständig war. Schrems wollte erwirken, dass Facebook untersagt werde, ihn betreffende Daten in die USA zu übermitteln und auf US-Servern von Facebook zu speichern.[5] Die irische Aufsichtsbehörde hatte sich auf die Rechtmäßigkeit der Datenübermittlung aufgrund des Safe Harbour-Abkommens gestützt und die Überprüfung der Beschwerde verweigert.

Der EuGH traf zum einen die Feststellung, dass die nationalen Datenschutzaufsichtsbehörden in Europa trotz der Safe Harbour-Entscheidung der Kommission[6] die Möglichkeit haben müssen, die Rechtmäßigeit der Datenübermittlung in die USA zu überprüfen.[7] Zudem stellte der EuGH fest, dass die Safe Harbour-Entscheidung der Kommission inhaltlich unzutreffend und daher ungültig sei.[8]

Datenübermittlungen aufgrund der Safe Harbour-Entscheidung sind daher unzulässig.

---

[2] 11. Tätigkeitsbericht des Beauftragten für den Datenschutz bei der Bayerischen Landeszentrale für neue Medien, S. 6
[3] Vgl. Entscheidung der EU-Kommission 2000/520
[4] EuGH Urteil vom 06.10.2015, C-362/14 (Schrems) in BayVBl. 2016, 193 ff.
[5] EuGH a.a.O. Rn. 28
[6] Entscheidung der Kommission vom 26.07.2000 gemäß der Richtlinie 95/46/EG des europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA (bekannt gegeben unter dem Aktenzeichen K [2000] 2441, ABl Nr. L 215 v. 25.08.2000 S. 7)
[7] EuGH a.a.O. Rn. 38-78
[8] EuGH a.a.O. Rn. 79-106

Die Mitgliedstaaten und die europäischen Datenschutzinstitutionen haben daraufhin die Gespräche mit den US-amerikanischen Behörden intensiviert, um politische, rechtliche und technische Lösungen für eine Nachfolgeregelung zu finden.

2.1.2 Datentransfers in die USA nach der Safe Harbour-Entscheidung des EuGH[9]

2.1.2.1 Standardvertragsklauseln und Binding Corporate Rules

Durch den Wegfall des Safe Harbour-Abkommens als Rechtsgrundlage für die Übermittlung personenbezogener Daten aus der Europäischen Union in die USA, haben einige Unternehmen kurzfristig Standardverträge als Rechtsgrundlage herangezogen. Auch wenn Standardvertragsklauseln oder Binding Corporate Rules formal von der o.g. EuGH-Entscheidung nicht betroffen waren, konnte eine Datenübermittlung auf dieser Grundlage angesichts der Feststellungen des EuGH nur noch schwerlich als materiell rechtmäßig angesehen werden.

2.1.2.2 EU-US Privacy Shield

Um die weiterhin laufend stattfindenden Datentransfers in die USA wieder auf eine tragfähige rechtliche Basis zu stellen, nahm die EU-Kommission unmittelbar nach der Safe Harbour-Entscheidung des EuGH Verhandlungen mit der US-Regierung auf, die letztlich am 12.07.2016 mit der bindenden Angemessenheitsentscheidung der Europäischen Kommission (2016/1250) das sogenannte EU-US Privacy Shield hervorbrachten. Dieses Privacy Shield stellt nunmehr in Form des o.g. Beschlusses eine neue Rechtsgrundlage für Datenübermittlungen in die USA dar. Seit dem 01.08.2016 können sich daher US-amerikanische Unternehmen beim dortigen Handelsministerium registrieren und unter Vorlage von diversen Nachweisen eine Zertifizierung beantragen. Sofern ein Unternehmen eine Zertifiizierung erhält, können personenbezogene Daten aus der Europäischen Union in die USA transferiert werden.[10]

Im Rahmen des o.g. Verfahrens war der EU zugesichert worden, den Zugriff auf personenbezogene Daten von EU-Bürgern aus Gründen der nationalen Sicherheit in den USA klaren Beschränkungen, Garantien und Aufsichtsmechanismen zu unterwerfen.[11] EU-Bürger könnten sich an einen Ombudsmann beim amerikanischen Außenministerium wenden, um Verstößen nachzugehen und prüfen zu lassen, ob ein Unternehmen rechtswidrig gehandelt habe.[12] Fragen zur Datenverarbeitung durch ein zertifiziertes US-Unternehmen könnten zunächst an das jeweilige US-Unternehmen gerichtet werden. Sollten die Fragen nicht durch das Unternehmen beantwortet werden oder weiterhin Bedenken hinsichtlich der Verarbeitung von Daten bestehen, kann eine Beschwerde bei der

---

[9] Vgl. oben 2.1.2: EuGH Urteil vom 06.10.2015, C-362/14 (Schrems); BayVBl. 2016, 193 ff.
[10] https://www.bfdi.bund.de/DE/Europa_International/International/Artikel/EU-US_PrivacyShield_Daten%C3%BCbermittlungenUSA.html?cms_templateQueryString=us+privacy+shield&cms_sortOrder=score+desc
[11] Vgl. Erwägungsgrund 28 des Beschlusses 2016/1250 vom 12. Juli 2016
[12] Nur möglich, wenn die nationale Aufsichtsbehörde keine Abhilfe schaffen kann (RDV 2016 S. 137)

zuständigen unabhängige Beschwerdestelle in den USA eingelegt werden. Als letzte Instanz steht die Möglichkeit eines Schiedsverfahrens in den USA zur Verfügung.[13] Gleichwohl steht zu befürchten, dass weiterhin eine flächendeckende und anlasslose Überwachung von EU-Bürgern stattfindet[14] und die mögliche Beschwerde bei dem o.g. Ombudsmann, einem Beamten des amerikanischen Außenministeriums, letztlich doch keine für die Wahrung europäischer Grundrechte hinreichende Rechtsschutzmöglichkeit darstellt, wie sie der EuGH in der o.g. Entscheidung für erforderlich gehalten hat.[15]

2.1.3 Transatlantische Handels- und Investitionspartnerschaft (TTIP)

Die EU und die USA verhandeln seit 2011 über ein Freihandelsabkommen, das unter dem Kürzel TTIP[16] bekannt ist und seit 2013 konkret mit dem Ziel diskutiert wurde, die Vorschriften und Regeln für die Wirtschaft in Europa und den USA langfristig so zu gestalten, dass sie zum Nutzen von Verbrauchern und Unternehmen besser miteinander vereinbar sind.

Es geht bei den Verhandlungen zu TTIP darum, Zölle und andere Handelsbarrieren im transatlantischen Handel zwischen der Europäischen Union (EU) und den Vereinigten Staaten von Amerika (USA) abzubauen und die Märkte auf beiden Seiten des Atlantiks zu öffnen.

Zu den Gesprächsthemen gehörten zwar bisher auch Fragen des zu beachtenden Datenschutzes. Ob diese Ansätze nach der o.g. Safe Harbour-Entscheidung des EuGH und neben dem erwähnten Privacy Shield noch eine eigenständige Bedeutung haben können, ist schwierig zu beantworten. Angesichts der unterdessen aufgetretenen Verhandlungshindernisse und der Haltung der neuen US-Regierung zu TTIP kann diese Frage aber zumindest derzeit als nachrangig eingestuft werden. Die vorerst letzte Verhandlungsrunde hat vom 3. bis 7.10.2016 in New York stattgefunden. Die Verhandlungen zu TTIPP ruhen seit Januar 2017.[17]

2.1.4 EU-Kanada-Wirtschafts- und Handelsabkommen (CETA)

Das umfassende Wirtschafts- und Handelsabkommen CETA (Comprehensive Economic and Trade Agreement) ist ein internationales Handelsabkommen zwischen der EU und

---

[13] https://www.bfdi.bund.de/DE/Europa_International/International/Artikel/EU-US_PrivacyShield_Daten%C3%BCbermittlungenUSA.html
[14] Vgl. die Stellungnahme der Art. 29 Datenschutzgruppe vom 13.04.2016
[15] Am 05.06.2018 hat das EU-Parlament für eine Aussetzung des Privacy-Shield-Abkommens votiert, da das Abkommen aus Sicht des Parlaments kein angemessenes Schutzniveau biete. Die Entscheidung des Parlaments ist für die EU-Kommission nicht bindend. Es erscheint aber unwahrscheinlich, dass sich die EU-Kommission der Forderung nach Nachbesserungen letztlich entziehen wird.
[16] http://www.bmwi.de/Redaktion/DE/Dossier/ttip.html
[17] https://www.bmwi.de/Redaktion/DE/Dossier/ttip.html

Kanada. Die EU und Kanada haben das Freihandelsabkommen am 30.10.2016 unterzeichnet.[18]
Eilanträge gegen CETA, die sich gegen eine Zustimmung des deutschen Vertreters im Rat der Europäischen Union zur Unterzeichnung, zum Abschluss und zur vorläufigen Anwendung des Freihandelsabkommens zwischen der Europäischen Union und Kanada richteten, wurden vom BVerfG abgelehnt.[19]
Damit das Abkommen vollständig in Kraft treten kann, muss es von den Parlamenten aller EU-Mitgliedstaaten ratifiziert werden. Der Bundestag müsste unter Beteiligung des Bundesrates nun ein entsprechendes Ratifikationsgesetz beschließen.[20]

In datenschutzrechtlicher Hinsicht kann das Abkommen interessant werden, da der Datenaustausch zwischen EU und Kanada z.B. im elektronischen Geschäftsverkehr zunehmen wird.

So heißt es in Art. 16.4 CETA beim Vertrauen in den elektronischen Geschäftsverkehr (Beschluss (EU) 2017/37 des Rates): „Jede Vertragspartei sollte Gesetze, sonstige Vorschriften oder Verwaltungsmaßnahmen zum Schutz der personenbezogenen Daten von Nutzern des elektronischen Geschäftsverkehrs einführen oder aufrechterhalten, wobei den internationalen Datenschutznormen einschlägiger internationaler Organisationen, bei denen beide Vertragsparteien Mitglied sind, gebührend Rechnung zu tragen ist."[21] Im Rahmen von Dialogen sollen sich die Vertragsparteien auch mit dem Schutz personenbezogender Daten befassen: „Schutz personenbezogener Daten und Schutz von Verbrauchern und Unternehmen vor betrügerischen und irreführenden Handelspraktiken im Bereich des elektronischen Geschäftsverkehrs.", Art. 16.6 Abs. 1 lit. d CETA (Beschluss (EU) 2017/37 des Rates).
Vor einem gegenseitigen Informationsaustausch über die Sicherheit von Konsumgütern und über getroffene Präventions-, Restriktions- und Korrekturmaßnahmen müssen die Vertragsparteien u.a. die Regeln zum Schutz personenbezogener Daten sicherstellen, Art. 21.7 Abs. 5 S. 2 CETA (Beschluss (EU) 2017/37 des Rates).

[18] Europäisches Amtsblatt vom 16.9.2017 (L 238/9)
[19] BVerfG, Urteil vom 13. Oktober 2016, 2 BvR 1368/16, 2 BvE 3/16, 2 BvR 1823/16, 2 BvR 1482/16, 2 BvR 1444/16
[20] https://www.bmwi.de/Redaktion/DE/Dossier/ceta.html
[21] Europäisches Amtsblatt vom 14.01.2017 (L 11/112)

2.2 Europäisches Recht

Das nationale Datenschutzrecht wird zunehmend durch Vorgaben der Europäischen Union geprägt. Grundlegende Vorgaben enthalten bereits die EU-Verträge, insbesondere die EU-Grundrechtecharta, die in Art. 8 ein Grundrecht auf Schutz personenbezogener Daten vorsieht. Darunter gaben die EU-Datenschutzrichtlinie[22] sowie die ePrivacy-Richtlinie (RL 2002/58/EG)[23] den zu beachtenden Rechtsrahmen vor. Unterdessen ist die EU-Datenschutz-Grundverordnung (DS-GVO) an die Stelle der Datenschutzrichtlinie getreten und ist seit Mai 2018 in allen EU-Mitgliedstaaten einheitlich verbindlich zu beachten.[24]

2.2.1 Vertrag von Lissabon

Der Vertrag von Lissabon, der am 13.12.2007 von den europäischen Staats- und Regierungschefs unterzeichnet worden ist, brachte nach dem Inkrafttreten am 01.12.2009 maßgebliche Änderungen für den Datenschutz mit sich. Durch ihn wurden die bislang geltenden Gemeinschaftsverträge grundlegend umgestaltet[25] und die Charta der Grundrechte in das europäische Primärrecht eingebunden. Für den Datenschutz ergeben sich daraus nicht unerhebliche Folgen.

In **Art. 16 Abs. 2 AEUV**[26] werden das Europäische Parlament und der Rat zum Erlass von Datenschutzvorschriften verpflichtet, deren Einhaltung von unabhängigen Behörden zu überwachen ist. Diese Verpflichtung gilt nicht nur für die Verarbeitung personenbezogener Daten durch europäische Institutionen, sondern auch für die Verarbeitung von Daten durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Unionsrecht fallen. Die inzwischen verabschiedete Datenschutz-Grundverordnung[27] ist eine Umsetzung dieser Vorgaben.

Die wohl wichtigste Änderung bestand jedoch in der Bezugnahme auf die Charta der Grundrechte. In **Art. 8 der Grundrechtecharta**[28] ist zum ersten Mal auf europäischer Ebene rechtsverbindlich ein **Grundrecht auf Datenschutz** normiert. Was dies für die

---

[22] RL 95/46/EG, ABl. EG vom 23.11.1995, Nr. L 281/31
[23] Im Telekommunikationsbereich wird die Datenschutzrichtlinie durch die im Jahr 2002 erlassene RL 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) ergänzt.
[24] Vgl. unten 2.2.2
[25] Die Europäische Union bestand bis zum Inkrafttreten des Vertrages von Lissabon aus dem Bereich der Europäischen Gemeinschaften (1.Säule), der gemeinsamen Außen- und Sicherheitspolitik (2.Säule) und der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (3.Säule).
[26] Vertrag über die Arbeitsweise der Europäischen Union
[27] Vgl. unten 2.2.2
[28] Art. 8 Schutz personenbezogener Daten
(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Geltung deutscher Grundrechte bedeutet, insbesondere ob die europäischen Grundrechte ein vergleichbares Schutzniveau gewährleisten,[29] ist nachwievor umstritten.[30.]

In diesem Zusammenhang wird jedoch wohl zunächst zu klären sein, welche Schutzgüter das europäische Recht im Auge hat. Denn ein vergleichbares europäisches Schutzniveau, das nach der bisherigen Rechtsprechung des Bundesverfassungsgerichtes die Voraussetzung für eine Verdrängung deutscher Grundrechtspositionen wäre, kann wohl nur entstehen, wenn die neu geschaffenen europäischen Rechte die gleichen Rechtsgüter schützen oder zumindest eine sehr ähnliche Zielrichtung verfolgen.[31]

2.2.2 EU-Datenschutz-Grundverordnung (DS-GVO)

2.2.2.1 Allgemeines

Die Europäische Kommission hat am 25.01.2012 den Entwurf einer europäischen Datenschutz-Grundverordnung[32] offiziell vorgelegt. Nachdem sich sowohl das Parlament als auch der Rat auf eine jeweils eigene Fassung verständigt hatten, begannen im Juni 2015 die Abstimmungsverhandlungen zwischen Rat, Parlament und Kommission (sogenannter Trilog), die im Dezember 2015 zu einer politischen Einigung geführt werden konnten. Die so gewonnenen Ergebnisse wurden im Laufe der nächsten Monate verbindlich beschlossen, so dass die neuen einheitlichen europäischen Regeln für den Datenschutz nach einer zweijährigen Übergangsphase, in der die nationalen Gesetzgeber ihre nationalen Regeln dem neuen Rechtszustand anpassen konnten, ab dem 25.05.2018 einheitlich in allen Mitgliedstaaten gelten.

Die DS-GVO wird wegen ihrer extraterritorialen Wirkung auch in Bezug auf Drittländer Anwendung finden. Wegen des Marktortprinzips werden auch außerhalb der EU niedergelassene Unternehmen die DS-GVO berücksichtigen müssen, sofern sie Personen innerhalb der EU Waren und Dienstleistungen anbieten oder deren Verhalten beobachten wollen, Art. 3 Abs. 1, 2 DS-GVO.

---

[29] Vgl. *Ronellenfitsch,* Der Vorrang des Grundrechts auf informationelle Selbstbestimmung vor dem AEUV, DuD, 2009, S. 451 ff.
[30] Johannes Masing, "Ein Abschied von den Grundrechten", SZ 29.01.2012. Der für Datenschutzfragen bisher zuständige Verfassungsrichter Prof. Masing vertrat in einer öffentlichen Stellungnahme die Auffassung, dass mit einer solchen Verordnung wohl auch deutsches Verfassungsrecht verdrängt würde, so dass die das Datenschutzrecht bisher maßgeblich im Sinne eines effektiven Grundrechtsschutzes prägende Rechtsprechung des Bundesverfassungsgerichtes dann möglicherweise weitgehend bedeutungslos würde.
[31] Ein Wechsel vom bundesdeutschen Grundrecht auf informationelle Selbstbestimmung zu einem europäischen Recht auf Datennutzung, das der Inhaber und Verarbeiter der Daten dem Betroffenen, auf den sich diese Daten beziehen, ggf. entgegenhalten kann, wie es gelegentlich aus der Datenschutz-Grundverordnung herausgelesen oder allgemein politisch gefordert wird, dürfte mit den weiterhin geltenden Grundrechten des Grundgesetzes nur schwer zu vereinbaren sein.
[32] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) – vom 25.01.2012, KOM (2012)/11 endgültig.

Die Datenschutz-Grundverordnung ersetzt die bisherige EU-Datenschutzrichtlinie 95/46/EC und bestimmt nun den Datenschutz in der EU weitestgehend. Das neue europäische Recht gilt unmittelbar, enthält aber für den öffentlichen Bereich größere Spielräume, die die nationalen Gesetzgeber für ihren Bereich individuell ausformen können.

Ein solcher Gestaltungsspielraum ergibt sich z.B. aus Art. 85 DS-GVO, der die Mitgliedstaaten auffordert, die neuen Datenschutzregeln mit den grundrechtlich verbürgten Freiheitsansprüchen von Rundfunk und Presse in Einklang zu bringen und den Mitgliedstaaten für diese Zwecke das Recht einräumt, Abweichungen und Ausnahmen von den meisten Regeln der DS-GVO vorzusehen. In Deutschland wurden für den Bereich des Rundfunks in § 9c und § 57 RStV neue Regeln für das sog. Medienprivileg erlassen.[33]

2.2.2.2 Inhalt der Verordnung

Für die Verarbeitung personenbezogener Daten gilt wie vormals schon im deutschen Recht der Grundsatz des Verbots mit Erlaubnisvorbehalt. Der Zweckbindungsgrundsatz und der Grundsatz der Datensparsamkeit stellen wichtige Prinzipien der DS-GVO dar. Personenbezogene Daten sollen nicht in einer mit dem ursprünglichen Erhebungszweck unvereinbaren Weise weiterverarbeitet werden. Grundsätzlich sollen die erfassten Daten auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt werden.
Es soll u.a. auch verschärfte Anforderungen an die Einwilligung zur Verarbeitung personenbezogener Daten geben,[34] so dass die DS-GVO insoweit einen robusten Individualdatenschutz vorsieht. Ferner soll es neue Rechte für Betroffene, wie u.a. ein umfassendes Auskunftsrecht, sowie erhöhte Transparenz- und Informationspflichten für die Verantwortlichen geben.[35]
Es soll das Prinzip des One Stop Shop gelten, so dass sich Verantwortliche und Betroffene künftig nicht mehr mit mehreren Datenschutzaufsichtsbehörden in verschiedenen Ländern auseinandersetzen müssen. Vielmehr soll in der Regel die Aufsichtsbehörde am Sitz der Hauptniederlassung federführend sein.[36]

Hervorzuheben ist auch die Stärkung der Befugnisse der Aufsichtsbehörden, insbesondere die Schaffung von Untersuchungs- und Abhilfebefugnissen sowie von effektiven Sanktionen.

Die Datenschutz-Grundverordnung räumt den Betroffenen auch erhebliche neue Rechte ein, was je nach Interessenlage unterschiedlich bewertet wird. Besonders hervorzuheben ist sicherlich der Ansatz, dem einzelnen Betroffenen ein „**Recht auf Vergessenwerden**" zu gewähren. Der EuGH hat dieses Recht in seiner Google-Spain-Entscheidung[37] bereits unter Geltung des alten Rechts konturiert. Der Verbraucher soll das Recht haben, ggf.

---

[33] Vgl. hierzu unten 2.3.6
[34] vgl. Art. 7 DS-GVO
[35] vgl. Art. 12 - 14 DS-GVO
[36] Dr. Peter Schantz, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, 1847
[37] Vgl. EuGH Urteil vom. 13.05.2014, C-131/12 und unten 2.2.3

nach einem Widerruf einer Einwilligung aber auch darüber hinaus vom Verantwortlichen die Löschung der ihn betreffenden Daten zu verlangen. In der Praxis wird dies wohl umfassend nur schwer umsetzbar sein, so dass dieses Recht möglicherweise doch nur einen qualifizierten Löschungsanspruch darstellen könnte.

Von Anfang an wurde das Ziel, eine Datenschutz-Grundverordnung zu schaffen, vor allem auch mit der Notwendigkeit begründet, künftig für einen **wirksamen Datenschutz** und die Einhaltung der europäischen Regeln insbesondere gegenüber international tätigen Firmen zu sorgen. Formell wurde diese Zielsetzung auch umgesetzt. Wenn Firmen gegen die neuen Regeln verstoßen, drohen ihnen massive Geldbußen von bis zu vier Prozent des weltweit erzielten Jahresumsatzes. Inwiefern die Androhung von Geldbußen in der Praxis tatsächlich die erwartete Bedeutung gewinnen, wird sich erst noch zeigen müssen.

Eine der zentralen Neuerungen ergibt sich aus dem europaweiten Ansatz der Datenschutz-Grundverordnung. Mit ihrer Einführung werden die rechtlichen Rahmenbedingungen für Fragen des Datenschutzes in ganz Europa weitgehend vereinheitlicht. Zudem sollen die nationalen Datenschutzbehörden zu zentralen Anlaufstellen für alle Bürger werden, so dass sich die Bürger nicht mehr um Fragen der örtlichen Zuständigkeit innerhalb Europas kümmern müssen. Und schließlich soll es für Unternehmen auch eine in allen Datenschutzfragen für dieses Unternehmen zuständige Aufsicht geben.

Damit dies alles auch gelingen kann, müssen die nationalen Datenschutzbehörden künftig sehr viel intensiver zusammenarbeiten. Die Zusammenarbeit zwischen diesen nationalen Behörden wird zu diesem Zweck institutionalisiert und erheblich verstärkt.

Die seit dem 1. Entwurf der Kommission in der Datenschutz-Grundverordnung vorgesehenen Zuständigkeiten der EU-Kommission **Delegierte Rechtsakte** zu erlassen, wurde zwar im Rahmen des Triloges eingeschränkt, sind aber immer noch in nennenswerter Anzahl vorhanden. Sie ermöglichen es, die zumeist sehr allgemein gehaltenen Vorgaben der Datenschutz-Grundverordnung zu konkretisieren.

2.2.2.3 Bewertung des Vorhabens

Trotz aller im Vorfeld geäußerten Bedenken und Zweifel kann die Einführung der Datenschutz-Grundverordnung als großer Erfolg Europas betrachtet werden. Die wesentlichen Zielsetzungen, ein einheitliches Datenschutzrecht für die gesamte EU zu schaffen, das aufgrund dieses Anwendungsbereiches auch Ausstrahlungswirkung deutlich darüber hinaus entfaltet, die Rechte der von der Digitalisierung in immer höherem Maße betroffenen Bürger Europas zu stärken, und dennoch einen verlässlichen und angemessenen Rechtsrahmen auch für die hier tätigen Unternehmen und Institutionen zu schaffen, die häufig auf die Verarbeitung von Daten angewiesen sind, die sich auf Dritte beziehen, sind erreicht worden, auch wenn nach wie vor zahlreiche Fragen noch offengeblieben oder nicht hinreichend geklärt erscheinen.

Letzteres liegt indes in der Natur der Sache, denn ein einheitlicher europäischer Rechtsrahmen für nahezu alle den Datenschutz betreffenden Rechtsfragen kann nur auf weitgehend sehr abstrakten Vorgaben beruhen, die daher zunächst viele ins Detail gehende Antworten auf konkrete Fragen offenlassen. Diese Antworten zu geben, ist die Aufgabe der Rechtsanwendung und insbesondere der Datenschutz-Aufsichtsinstitutionen, denen durch die DS-GVO gerade auch in dieser Hinsicht zahlreiche Aufgaben zugewiesen sind.

Betrachtet man nur die Fülle der deutlich im dreistelligen Bereich liegenden allein in Deutschland aufgrund der Einführung der DS-GVO anzupassenden Gesetze, mag man die Größe der bestehenden Aufgabe hieraus jedenfalls in Ansätzen ermessen können, denn die meisten der bisher in Spezialgesetzen enthaltenen auf das jeweilige Fachgebiet bezogenen gesetzgeberischen Entscheidungen müssen nun auf die neue Rechtslage bezogen aus der Datenschutz-Grundverordnung und ihren abstrakten Vorgaben abgeleitet werden. Dass die so erforderlich gewordenen Abwägungen nicht für alle Detailfragen sofort gewissermaßen aus dem Stand gelingen können, sondern in vielen Fällen einer hinreichenden Prüfung und gegebenenfalls auch eingehenden Diskussion bedürfen, sollte bei dieser Sachlage unschwer einsichtig sein.

Dies gilt insbesondere angesichts der zu der DS-GVO schon im Vorfeld von unterschiedlichsten Interessengruppen geäußerten Erwartungen, welche in ihrem Grundverständnis von höchst unterschiedlichen Positionen ausgingen. Diese unterschiedlichen Ansichten wie auch die Interessen der Internetwirtschaft einerseits und die ebenfalls sehr vehement vertretenen Vorstellungen von einem robusten individuellen Grundrechtsschutz der Betroffenen andererseits zu einem sinnvollen Ausgleich zu bringen, wird eine der wesentlichen Aufgaben der künftigen Rechtsanwendung sein.

Zu den Aufgaben der Datenschutzaufsicht wird es daher vor allem auch gehören, diese Zusammenhänge verständlich zu schildern und die sich daraus ergebenden Notwendigkeiten zu erklären, sowie bei den Betroffenen für die erforderliche Geduld zu werben. Dies gilt insbesondere auch für den Bereich des Rundfunkdatenschutzes, in welchem neben der DS-GVO auch nahezu alle anderen staatsvertraglichen und bayerischen Rechtsvorgaben neu geschaffen oder doch maßgeblich umgestaltet wurden. Da die DS-GVO jedoch nach den bisherigen Erfahrungen für die allermeisten Fragestellungen brauchbare Lösungsansätze bereithält, die lediglich einer sinnvollen Auslegung im Hinblick auf den jeweiligen Einzelfall bedürfen, sollte es im Laufe der Zeit möglich sein, die sicherlich an vielen Stellen noch nicht abschließend entschiedenen Grundsatzfragen zu klären, daraus ein gefestigtes Verständnis vom neuen europäischen Datenschutzrecht zu entwicklen, und auf dieser Basis auftretende Praxisfragen rasch und überzeugend beantworten zu können.

2.2.3 Zulässigkeit der Vorratsdatenspeicherung

In einer sich zunehmend digitalisierenden Gesellschaft spielt die Möglichkeit, die in den verschiedensten Lebensbereichen entstehenden personenbezogenen Daten nutzen zu

können, eine immer größere Rolle. Daher liegt der Gedanke nahe zu verlangen, für bestimmte Anliegen des Gemeinwohls ohnehin angefallene Daten für einen bestimmten Zeitraum aufzubewahren oder auch die ansonsten ggf. nicht stattfindende Speicherung von Daten aus bestimmten Nutzungszusammenhängen verbindlich vorzusehen. Solches wurde mit der Richtlinie 2006/24/EG[38] vom 15.03.2006 den EU-Mitgliedsstaaten aufgegeben, die dafür Sorge tragen sollten, dass von Anbietern von Telekommunikationsdiensten Verbindungsdaten verschiedenster Kategorien mindestens sechs Monate auf Vorrat, also ohne dass die Betroffenen hierzu einen Anlass geboten hätten, gespeichert werden.[39] Erste Klagen gegen diese Richtlinie hatte der EuGH noch zurückgewiesen,[40] dabei aber Aussagen zu einer möglichen Verletzung von Grundrechten bewusst vermieden.[41]

In Deutschland wurde die o.g. Richtlinie erstmals im Jahr 2007 umgesetzt[42], die Umsetzung aber vom Bundesverfassungsgericht[43] verworfen.[44] Eine Neuregelung scheiterte zunächst an Auffassungsunterschieden in der damaligen Bundesregierung[45], wurde dann aber doch zur Vermeidung von Zwangsgeldern beschlossen.[46] Im April 2014 entschied der EuGH, dass die o.g. Richtlinie gegen die EU-Grundrechtecharta verstoße[47], weil sie einen unzulässigen Eingriff insbesondere in die Grundrechte des Telekommunikationsgeheimnisses, auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten darstelle. Im Mai 2015 wurde dennoch der Entwurf eines Gesetzes zur Einführung einer Speicherpflicht für Verkehrsdaten vorgelegt[48], der zwar intensiv kritisiert[49], dennoch aber beschlossen wurde[50] und am 18.12.2015 in Kraft trat.[51]

---

[38] ABl. EG vom 15.03.2006, Nr. L 105/54
[39] Vgl. Art. 3 i.V.m Art. 6 der RL 2006/24/EG
[40] EuGH Urteil vom 10.02.2009, C-301/06
[41] Der EuGH hielt es für gerechtfertigt, dass der Gemeinschaftsgesetzgeber das Ziel, das Funktionieren des Binnenmarkts zu schützen, durch den Erlass von solchen Harmonisierungsvorschriften verfolge.
Warum eine solche Verpflichtung wirklich für das Funktionieren des Binnenmarktes erforderlich sein soll, wurde nicht begründet. Zudem harmonisierte die Richtlinie keineswegs nur Speicherungspflichten, sondern führte massiv in die Datenschutzrechte der Gemeinschaftsbürger eingreifende Verpflichtungen auch für die Länder verbindlich ein, in denen es bis dahin keine derartige Verpflichtung gab und in denen zudem berechtigte Zweifel bestanden, ob deren nationale Gesetzgeber eine solche Verpflichtung überhaupt einführen könnten, geschweige denn würden.
[42] Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, BGBl. 2007 I Nr. 70 S. 3198 ff.
[43] BVerfG Urteil vom 02.03.2010, BVerfGE 125, 260 ff.
[44] Das Gericht war der Ansicht, der Gesetzgeber sei seinem Auftrag nicht nachgekommen, "die Ermächtigung zur Massenspeicherung von Telekommunikationsdaten mit angemessenen Schutzmechanismen zu flankieren, weshalb die momentane deutsche Umsetzung der Richtlinie verfassungswidrig und nichtig sei", vgl. K&R 2010, S. 220.
[45] Vgl. Möstl, Zeitschrift für Rechtspolitik 2011, S. 226
[46] Koalitionsvertrag 16.12.2013, S. 102, 103, "Dabei sollte ein Zugriff auf die gespeicherten Daten nur bei schweren Straftaten und nach Genehmigung durch einen Richter sowie zur Abwehr akuter Gefahren für Leib und Leben erfolgen."
[47] Vgl. EuGH Urteil vom 08.04.2014, C-293/12 und C-594/12; K&R 2014, 405 ff.
[48] BR-Drs. 249/15
[49] Umlaufentschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09.06.2015
[50] BT-Drs. 186391
[51] BGBl. 2015 I Nr. 51 S. 1324 ff.

Mit Urteil vom 21.12.2016[52] hat der EuGH sich nochmals mit nationalen Regeln zur Vorratsdatenspeicherung befasst und diesmal schwedische und britische Vorschriften zur Vorratsdatenspeicherung für ungültig erklärt, die eine allgemeine und unterschiedslose Speicherung von Daten vorsahen. Dabei hat er aber betont, dass eine vorbeugende, gezielte Vorratsdatenspeicherung zum allgemeinen Zweck der Bekämpfung schwerer Straftaten zulässig sei, sofern eine solche Speicherung hinsichtlich der Kategorien von zu speichernden Daten, der erfassten Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Speicherung auf das absolut Notwendige beschränkt sei, und diese Einschränkung der Vertraulichkeit der Kommunikation nicht zur Regel werde.[53] Das OVG-NRW setzte mit Beschluss vom 22. Juni 2017 Verpflichtungen aus dem o.g. Gesetz zur Einführung einer Speicherpflicht für Verkehrsdaten insbesondere mit Blick auf die Rechtsprechung des EuGH aus.[54] In der Folge setzte die Bundesnetzagentur die o.g. Pflicht zur Vorratsdatenspeicherung aus diesem Gesetz bis zur Entscheidung im Hauptsacheverfahren faktisch aus.[55]

2.2.4 Richtlinie 2009/136/EG[56]

Am 25.11.2009 haben das Europäische Parlament und der Rat der Europäischen Union mit der Richtlinie 2009/136/EG (sog. Cookie-Richtlinie) u.a. Vorgaben der sogenannten ePrivacy-Richtlinie (2002/58/EG)[57] verschärft und Informationspflichten für den Fall einer Verletzung des Schutzes personenbezogener Daten geschaffen,[58] die über die vorherigen Vorgaben[59] hinausgehen.[60] Zudem enthält die RL 2009/136/EG auch die Vorgabe[61], eine Speicherung von Informationen oder den Zugriff auf Informationen auf dem Endgerät eines Teilnehmers oder Nutzers im Wesentlichen nur zu gestatten, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen seine Einwilligung gegeben hat.

---

[52] EuGH Urteil vom 21.12.2016, C-203/15 und C-698/15.
[53] Vgl. auch EuGH Pressemitteilung Nr. 145/16. Wegen der weitreichenden Folgen einer solchen Speicherverpflichtung hält der EuGH zudem materielle und verfahrensrechtliche Voraussetzungen der Nutzung solcher Daten für erforderlich wie objektive Anhaltspunkte im konkreten Fall, die Freigabe durch ein Gericht oder eine unabhängige Stelle, die Speicherung der Daten im Unionsgebiet, die Information der Betroffenen und die unwiderrufliche Löschung der Daten nach Fristablauf.
[54] OVG NRW, Beschluss vom 22.06.2017, 13 B 238/17
[55] https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/ AnbieterpflichtenOeffentlicheSicherheit/Umsetzung110TKG/VDS_113aTKG/VDS.html, Stand 28.06.2017
[56] RL 2009/136/EG zur Änderung der RL 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der RL 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz
[57] Datenschutzrichtlinie für elektronische Kommunikation, RL 2002/58/EG
[58] z.B. hat der Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste nach dem neuen Art. 4 Abs. 3 der ePrivacy-RL im Falle einer Verletzung des Schutzes personenbezogener Daten unverzüglich die zuständige nationale Behörde und darüber hinaus auch die betroffenen Personen von der Verletzung zu benachrichtigen, wenn anzunehmen ist, dass diese durch die Verletzung des Schutzes personenbezogener Daten in ihrer Privatsphäre beeinträchtigt werden.
[59] z.B. in § 42a BDSG (alt), § 15a TMG und § 93 Abs. 3 TKG
[60] Umsetzung der RL in der Novelle zum TKG vom 09.05.2012, BGBl. 2012 I Nr. 19 S. 958 ff.
[61] Über eine Änderung von Art. 5 Abs. 3 der RL 2002/58/EG, der sog.ePrivacy-Richtlinie

ePrivacy-Richtlinie und Cookie-Richtlinie sollen nunmehr durch eine ePrivacy-Verordnung abgelöst werden. Am 10.01.2017 hat die Kommission einen ersten Entwurf für die ePrivacy-Verordnung veröffentlicht.[62] Ursprünglich sollte die ePrivacy Verordnung zeitgleich mit der EU-Datenschutz-Grundverordnung (DS-GVO) in Kraft treten, befindet sich aber noch im europäischen Gesetzgebungsverfahren. Die ePrivacy-Verordnung soll u.a. den Datenschutz bei elektronischen Kommunikationsvorgängen regeln und wohl auch auf internetbasiete Kommunikationsdienste wie Messenger-Dienste oder Web-E-Mailanbieter anwendbar sein. Die ePrivacy-Verordnung soll die DS-GVO ergänzen und präzisieren.[63]

2.2.5 Urteil des EuGH zu Google Spain

Mit dem Urteil in Sachen Google Spain[64] hat der EuGH Google verpflichtet, Links auf von Dritten veröffentlichte Informationen in den Ergebnislisten ihrer Suchmaschine unter bestimmten Voraussetzungen zu entfernen.[65] Zudem hat der EuGH in diesem Zusammenhang verschiedene Grundaussagen von beträchtlicher Reichweite getroffen, die zwar formal auf der Anwendung der europäischen Datenschutzrichtlinie (95/46/EG) beruhten, wegen ihrer Grundsätzlichkeit aber auch noch unter der veränderten Rechtslage gültig sein dürften.[66]

Hierzu gehört insbesondere die Feststellung, dass das Betreiben einer Suchmaschine, die automatisch im Internet veröffentlichte Informationen aufspürt, ein eigenes Erheben von Daten darstellt, was den Anwendungsbereich des Datenschutzrechtes für die Kerntätigkeit einer Suchmaschine eröffnet. Der Betreiber der Suchmaschine entscheide über die Zwecke und Mittel der Datenverarbeitung und sei daher für die Verarbeitung verantwortlich. Zudem wurde festgestellt, dass diese Verarbeitung im Rahmen der Tätigkeit einer in der EU befindlichen Niederlassung erfolgt, wenn diese Niederlassung die Aufgabe der Vermarktung der Werbeflächen der Suchmaschine wahrnimmt.

Schließlich wurde eine Verpflichtung des Suchmaschinenbetreibers bejaht, Verweise auf von Dritten veröffentlichte Internetseiten mit personenbezogenen Informationen zu entfernen, wenn sich bei Würdigung aller Umstände des Einzelfalls ein überwiegendes Individualinteresse des Betroffenen an der Löschung ergibt. Dies gilt gegebenenfalls auch dann, wenn die betreffende Veröffentlichung auf den verlinkten Internetseiten als solche rechtmäßig ist[67], weil die Rolle des Internets und der Suchmaschinen in einer modernen

---

[62] https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications
[63] Kristin Benedikt, Die geplante ePrivacy-Verordnung und ihr Verhältnis zur DS-GVO und zum TMG, Datenschutzberater 4/2018, S. 80 ff.
[64] EuGH Urteil vom 13.05.2014, C-131/12
[65] Ein spanischer Staatsbürger hatte sich dagegen gewandt, dass bei der Eingabe seines Namens die Suchmaschine von Google in der Ergebnisliste auf Informationen hinwies, die seinerzeit zwar zutreffend, unterdessen aber vollständig erledigt waren.
[66] Vgl. oben 2.2.2.2, insbesondere zum Recht auf Vergessen aus Art. 17 DS-GVO
[67] EuGH Urteil vom 13.05.2014, C-131/12 Rdnr. 62

Gesellschaft eine besondere ist und den in den Ergebnislisten enthaltenen Informationen Ubiquität verleiht.

2.2.6 Vorlage an den EuGH zur Einbindung des „Gefällt mir"-Buttons

Das Oberlandesgericht (OLG) Düsseldorf hat dem Gerichtshof der Europäischen Union (EuGH) am 19.01.2017 Fragen zur datenschutzrechtlichen Zulässigkeit des Facebook „Like"-Buttons und der Einbindung eines entsprechenden „Gefällt mir"-Plugins vorgelegt.[68] Dabei soll geklärt werden, ob Webseiten-Betreiber den Facebook „Like"-Button in datenschutzrechtlich zulässiger Weise einbinden können, obwohl dadurch automatisch Nutzerdaten an Facebook übertragen werden. Die Verbraucherzentrale NRW hatte gegen einen Modekonzern, der ein solches „Gefällt mir"-Plugin von Facebook in seinen Internetauftritt integrierte, Unterlassungsklage erhoben, weil über das Plugin bereits beim einfachen Aufrufen der konzerneigenen Webseite Daten über das Surfverhalten eines jeden Nutzers an Facebook weitergegeben würden. Hierin sah die Verbraucherzentrale einen Verstoß gegen das Wettbewerbsrecht und das (alte) Datenschutzrecht.[69]

Das entsprechende Plugin ist auf vielen Webseiten von Unternehmen und Privatpersonen zu finden und überträgt bereits beim Besuch dieser Webseiten automatisch Daten der Besucher an Facebook, auch wenn diese selbst keine Facebook-Nutzer und dort auch nicht registriert sind, und vor allem auch ohne dass dies für die Nutzer erkennbar wäre. Mit Hilfe der gesetzten Cookies können u.a. IP-Adressen wiedererkannt und Surfprofile der Nutzer angelegt werden. Wenn ein Nutzer darüberhinaus bei Facebook registriert und auch eingeloggt ist, kann Facebook genau nachvollziehen, welche Internetseiten von diesem Nutzer besucht werden. Es besteht die Gefahr einer Überwachung von Nutern im Internet.[70] Auch wenn die Vorlagefrage noch die alte Rechtslage betrifft, ist zu erwarten, dass sich die Entscheidung auch auf die neue Rechtslage wird übertragen lassen.

2.2.7 Personenbezug von IP Adressen

Einrichtungen des Bundes speichern bei Besuchen auf ihren Webseiten die IP-Adressen der Besucher auch noch nach Ende des Seitenbesuchs und damit länger als technisch zwingend erforderlich. Dagegen wendete sich der schleswig-holsteinische Abgeordnete der Piratenpartei Patrick Breyer. Er sieht in der Speicherung eine unzulässige Überwachung der Webseiten-Nutzer. Die beklagte Bundesrepublik Deutschland als Webseiten-Betreiberin hält die Speicherung der IP-Adressen dagegen für zulässig: Sie argumentiert, nur so technische Maßnahmen ergreifen zu können, wenn ihre Internetangebote angegriffen würden, und gegebenenfalls strafrechtliche Schritte gegen die Angreifer einleiten zu können.

---

[68] OLG Düsseldorf, Beschluss vom. 19.01.2017, I-20 U 40/16
[69] LG Düsseldorf, Urteil vom 09.03.2016, 12 O 151/15
[70] OLG Düsseldorf, Beschluss vom. 19.01.2017, I-20 U 40/16, u.a. Rn. 45

Der Bundesgerichtshof setzte das bei ihm anhängige Verfahren zunächst aus[71] und legte dem Europäischen Gerichtshof zwei Fragen zur Auslegung der EG-Datenschutz-Richtlinie zur Vorabentscheidung vor.
Der EuGH stellte hierauf fest, dass dynamische IP-Adressen, die von einem Anbieter von Online-Mediendiensten beim Zugriff einer Person auf eine allgemein zugängliche Homepage gespeichert werden, für den Anbieter ein personenbezogenes Datum darstellen,[72] wenn er über rechtliche Mittel verfügt, die es ihm ermöglichen, die betreffende Person anhand der Zusatzinformationen bestimmen zu lassen.[73]
Nachdem der EuGH mit Urteil vom 19. Oktober 2016 die Fragen beantwortet hatte,[74] entschied auch der BGH mit Urteil vom 16. Mai 2017, dass eine dynamische IP-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff einer Person auf eine Internetseite, die dieser Anbieter allgemein zugänglich macht, gespeichert wird, für den Anbieter ein (geschütztes) personenbezogenes Datum im Sinne von § 12 Abs. 1 und 2 TMG i.V.m. § 3 Abs. 1 BDSG (alt) darstellt.[75]

Damit dürfte auch für die Rechtslage nach der DS-GVO feststehen, dass personenbeziehbare und damit im Rechtssinn personenbezogene Daten jedenfalls dann vorliegen, wenn der Verantwortliche auf rechtlich zulässige Weise die Personen ausfindig machen kann, auf welche sich die gespeicherten Daten beziehen. Da diese Voraussetzung im zu entscheidenden Fall vorlag, mussten sich die Gerichte nicht zu der Frage äußern, ob dies auch dann gelten würde, wenn die Feststellung der maßgeblichen Person, auf welche sich die Daten beziehen, zwar möglich ist, die dafür erforderlichen Maßnahmen in Europa aber nicht zulässig sind.

---

[71] BGH, Beschluss vom 28.10.2014, VI ZR 135/13
[72] EuGH, Urteil vom 19.10.2016, C 582/14
[73] Für die Zulässigkeit der Verarbeitung dieser personenbezogenen Daten stellte der EuGH zudem fest, dass im Einzelfall eine Interessenabwägung möglich sein müsse, wie dies in Art.7 lit. f der Datenschutzrichtlinie vorgesehen sei. Die personenbezogenen Daten dürften danach länger gespeichert werden, wenn nicht die Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Person die berechtigten Interessen des Webseiten-Betreibers überwiegen. Auf Seiten des Webseiten-Betreibers sei insbesondere das Interesse zu berücksichtigen, die generelle Funktionsfähigkeit des Internetangebots zu gewährleisten. Eine Abwägung konnte im Streitfall allerdings nicht abschließend vorgenommen werden, da bisher keine hinreichenden Feststellungen dazu getroffen worden waren, ob die Speicherung der IP-Adressen des Klägers über das Ende eines Nutzungsvorgangs hinaus erforderlich sind.
[74] EuGH, Urteil vom 19.10.2016, C 582/14
[75] BGH, Urteil vom 16.05.2017, IV ZR 135/13. Ferner entschied der BGH, dass ein Anbieter von Online-Mediendiensten personenbezogene Daten eines Nutzers dieser Dienste ohne dessen Einwilligung über das Ende eines Nutzungsvorgangs hinaus erheben und verwenden darf, soweit die Erhebung und ihre Verwendung erforderlich sind, um die generelle Funktionsfähigkeit des Dienistes zu gewährleisten und bei einer Interessensabwägung nicht die Rechte und Freiheiten des Nutzers überwiegen.

2.3 Bundesrecht

Eine Anpassung aller Bundesgesetze mit Regelungen zum Datenschutz an die mit der DS-GVO eingetretenen Rechtsänderungen war im Berichtszeitraum aus unterschiedlichen Gründen gescheitert. Mit dem Datenschutz-Anpassungs- und Umsetzungsgesetz EU (DSAnpUG-EU)[76] wurden jedoch maßgebliche Änderungen v.a. im BDSG, im Bundesverfassungsschutzgesetz und BND-Gesetz vorgenommen. Ähnliches soll im Hinblick auf weitere 154 Bundesgesetze nach dem Willen des Bundestages alsbald in Angriff genommen werden. Ein entprechender Entwurf zu einem zweiten Datenschutz-Anpassungs- und Umsetzungsgesetz EU (2. DSAnpUG-EU) wurde am 01.10.2018 veröffentlicht.[77]

2.3.1 Bundesdatenschutzgesetz (BDSG)

Im Koalitionsvertrag von 2013 hatten sich CDU, CSU und SPD darauf geeinigt, die Verhandlungen zur Europäischen Datenschutz-Grundverordnung mit dem Ziel zu verfolgen, das vorhandene nationale Datenschutzniveau zu erhalten und über das europäische Niveau hinausgehende Standards zu ermöglichen.[78]

Mit der Einführung der DS-GVO wurden die meisten Regelungen des BDSG wegen des Anwendungsvorranges des Europarechtes obsolet, so dass das BDSG grundlegend überarbeitet werden musste, was mit dem Datenschutz-Anpassungs- und Umsetzungsgesetz EU (DSAnpUG-EU)[79] geschah. Das neue BDSG enthält seither v.a. Regelungen zu den Bereichen, die das Europarecht ausspart, bzw. in denen dieses den Mitgliedstaaten Regelungsspielräume eröffnet. Dies gilt z.B. für den Beschäftigtendatenschutz, der abgesehen von sehr allgemein gehaltenen Vorgaben der Regelung durch die Mitgliedstaaten überlassen wurde.[80] Die bisherige Regelung zum Beschäftigtendatenschutz wurde in § 26 BDSG n.F. fortgeschrieben.[81]

Daneben enthält des neue BDSG in den §§ 17 bis 19 Vorgaben zur Zusammenarbeit der verschiedenen Datenschutzaufsichtsinstitutionen vor allem im Hinblick auf den mit der DS-GVO geschaffenen Europäischen Datenschutzausschuss. Dabei wurden auch Regelungen für die Zusammenarbeit der vom Staat getragenen Datenschutzaufsichtsinstitutionen mit den für den Bereich des Medienprivilegs und der kirchlichenen Selbstverwaltung eingerichteten spezifischen Aufsichtsbehörden geschaffen, vgl. § 18 Abs. 1 BDSG.

---

[76] BGBl. I 2017,2097
[77] BT DS 19/4674
[78] Koalitionsvertrag vom 16.12.2013 S. 50
[79] BGBl. I 2017,2097
[80] Vgl. Art. 88 DS-GVO und Erwägungsgrund Erwägungsgrund 155
[81] Dr. Peter Schantz, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, 1841

Leider wurde dabei übersehen, dass das Grundgesetz aus Gründen des das Rundfunkverfassungsrecht durchziehenden Gebotes der Staatsferne[82] auch staatsfern getragene Datenschutzaufsichtsinstitutionen erforderlich macht, deren Zuständigkeit sich keineswegs im Anwendungsbereich des Medienprivilegs erschöpft. Diese staatsfernen Aufsichtsinstitutionen besitzen häufig die gleichen Aufgaben und Befugnisse nach Art. 57 und 58 DS-GVO wie die von Bund und Ländern getragenen Datenschutzbehörden und stellen in gleicher Weise nach Art. 51 DS-GVO für nahezu alle mit der DS-GVO verbundenen Rechtsfragen zuständige Aufsichtsbehörden dar. Sie haben dann zwar auch die Aufgaben einer sog. spezifischen Aufsichtsbehörde; ihre Aufgaben erschöpfen sich aber nicht in diesen, sondern umfassen das nahezu gleiche Spektrum wie der Aufgabenbereich der vom Staat getragenen Datenschutzaufsichtsbehörden, bzw. gehen sogar darüber hinaus, da sie i.d.R. auch im Bereich des Medienprivilegs zuständig sind, der den staatlichen Datenschutzaufsichtsbehörden gerade verschlossen ist.

2.3.2 Telemediengesetz (TMG) und Telekommunikationsgesetz (TKG)

Die im Berichtzeitraum erfolgten Änderungen des TKG und TMG entfalteten keine datenschutzrechtlichen Wirkungen.

Anpassungen des TMG an die DS-GVO wurden bislang nicht in die Wege geleitet, womit das TMG zwar im Berichtszeitraum noch in Kraft war, mit dem Inkrafttreten der DS-GVO aber in weiten Teilen von dieser überlagert wird. Etwas anderes gilt nur soweit das TMG die ePrivacy-Richtlinie (2002/58/EG)[83] umsetzt. In welchem Umfang dies der Fall ist, ist umstritten.[84] Die in der Datenschutzkonferenz (DSK) zusammengefassten staatlichen Datenschutzbehörden des Bundes und der Länder vertreten die Auffassung, dass die Datenschutzregeln des TMG, also die §§ 12 ff. TMG, ab 25.05.2018 nicht mehr anwendbar sind, weil es gerade an dieser Umsetzung fehle.[85]

An die Stelle der ePrivacy-Richtlinie soll in absehbarer Zeit die ePrivacy-Verordnung treten, die ursprünglich zeitgleich mit der DS-GVO in Kraft treten sollte. Das europäische Gesetzgebungsverfahren dürfte aber noch geraume Zeit in Anspruch nehmen, so dass mit einem Inkrafttreten nicht vor 2020 zu rechnen sein dürfte. Danach dürften aber auch die bisher im Hinblick auf das TMG bestehenden Zweifelsfragen geklärt sein, da diese neuen Vorgaben dann als europäische Verordnung einen Anwendungsvorrang vor nationalem Recht genießen.

---

[82] Diese Überlegungen dürften für den Bereich der Presse prinzipiell ebenso zutreffend sein, auch wenn sich die aktuelle Ausgestaltung dort erheblich von den Gegebenheiten im Rundfunk unterscheidet.
[83] Die Richtlinie (2002/58/EG) gilt wegen Art. 95 DS-GVO auch künftig, vgl. oben 2.2.4
[84] Kristin Benedikt, Die geplante ePrivacy-Verordnung und ihr Verhältnis zur DS-GVO und zum TMG, Datenschutzberater 4/2018, S. 80 ff.
[85] DSK Positionspapier vom 26.04.2018, Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018

2.3.3 IT-Sicherheitsgesetz

Das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) wurde am 12.06.2015 vom Bundestag beschlossen und ist nach Zustimmung des Bundesrats am 25.07.2015 in Kraft getreten.[86]

Das Gesetz verpflichtet Betreiber kritischer Infrastrukturen[87], die von so hoher Bedeutung für das Funktionieren des Gemeinwesens sind, dass deren Ausfälle erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit mit sich bringen können (vgl. § 2 Abs. 10 BSIG).

Das BSIG wird durch Rechtsverordnungen konkretisiert. So gilt für Betreiber kritischer Infrastrukturen aus den Bereichen Energie, Informationstechnik und Telekommunikation sowie Ernährung und Wasser die KRITIS-Verordnung vom 3. Mai 2016.[88] Diese Rechtsverordnung legt fest, welche Unternehmen im Sinne des Gesetzes zu den kritischen Infrastrukturen zählen.

Die maßgeblichen Verpflichtungen des Gesetzes für die Betreiber kritischer Infrastrukturen bestehen darin, IT-Sicherheit nach dem Stand der Technik umzusetzen und deren Einhaltung regelmäßig nachzuweisen. Auch eine Meldepflicht für Störfälle wurde eingeführt. Zudem erhielten Telekommunikationsdiensteanbieter das Recht, Bestands-und Verkehrsdaten von Teilnehmern und Nutzern zu erheben und zu verwenden, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen.[89] Aus datenschutzrechtlicher Sicht besteht eine gewisse Problematik darin, dass so Informationen unabhängig von einer Zweckbindung gespeichert werden dürfen, und das Gesetz auch keine Höchstspeicherdauer festlegt[90].

2.3.4 Datenhehlerei (§ 202d StGB)

Am 17.12.2015 wurde mit dem neuen § 202d StGB der Straftatbestand der Datenhehlerei geschaffen.[91]

Begründet wurde dies damit, dass mit der sich rasant entwickelnden Informationstechnologie der Handel mit rechtswidrig erlangten digitalen Daten wie z.B. Kreditkartendaten oder Zugangsdaten zu Onlinebanking, E-Mail-Diensten oder sozialen Netzwerken immer

---

[86] BGBl. 2015 I Nr. 31 S. 1324 ff.
[87] Gemeint sind solche aus den Bereichen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen, vgl. § 2 Abs. 10 BSIG.
[88] BGBl 2016 I Nr. 20, S. 958 ff.
[89] Vgl. § 100 Abs.1 TKG
[90] Vgl. Rath/Kuss/Bach in K&R 2015, 439; https://www.datenschutzzentrum.de/artikel/920-Entwurf-eines-Gesetzes-zur-Einfuehrung-einer-Speicherpflicht-und-einer-Hoechstspeicherfrist-fuer-Verkehrsdaten.html#extended S. 12
[91] BGBl 2015 I Nr. 51, S. 2227

mehr an Umfang gewonnen habe. Die Täter würden häufig selbst keine unmittelbaren Vermögensverfügungen vornehmen, sondern über Webportale auf intensive Weise Handel mit den ausgespähten Daten betreiben. Die Taten seien nur in Teilbereichen von bestehenden Strafnormen gedeckt, so dass der Schutz des Bürgers und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[92] den neuen Tatbestand erfordere.
Die oben geschilderten tatsächlichen Annahmen können aus der Praxis der Landeszentrale bestätigt werden. Es bleibt zu hoffen, dass die Einführung des neuen Straftatbestandes und eine entsprechend konsequente Anwendung die oben genannten Schutzziele erreichen. Allerdings werden von Pressevertretern die in Abs. 3 Nr 2 enthaltene Privilegierung von Journalisten als in der Ausgestaltung mangelhaft angesehen, weshalb derzeit eine Verfassungsbeschwerde anhängig ist.[93]

2.3.5 Verbandsklagerecht

Am 24.02.2016 ist das „**Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts**" in Kraft getreten.[94] Es enthält schwerpunktmäßig Änderungen des Unterlassungsklagengesetzes (UKlaG) und des Bürgerlichen Gesetzbuches (BGB).
Neu ist die Aufnahme von Datenschutzvorschriften in den Katalog der Verbraucherschutzgesetze, deren Missachtung nach § 2 Abs. 1 UKlaG Unterlassungs- und Beseitigungsansprüche entstehen lässt.
Den genannten anspruchberechtigten Stellen[95] – z.B. Verbraucherschutzverbände – stehen künftig Unterlassungs- und Beseitigungsansprüche zu, wenn ein Unternehmen personenbezogene Daten eines Verbrauchers entgegen den datenschutzrechtlichen Bestimmungen verarbeitet und die Verarbeitung einem kommerziellen Zweck dient.[96]
Somit besteht die Möglichkeit, dass Verbraucherverbänden für den einzelnen Betroffenen Klage einlegen (Verbandsklage). Die Durchsetzbarkeit von Ansprüchen Betroffener wird erleichtert, wohingegen der Verantwortliche selbstständig nachweisen und dokumentieren muss, dass seine Datenverarbeitung datenschutzkonform erfolgt.[97] Allerdings ist der Anwendungsbereich auf bestimmte datenschutzrechtliche Verstöße beschränkt. Die vorliegende Reform des UKlaG dürfte mit der DS-GVO vereinbar sein,[98] zumal auch Art. 80 Abs. 2 DS-GVO vorsieht, dass die Mitgliedstaaten ein solches Verbandsklagerecht einrichten können, da es der EU ein Anliegen war, die Durchsetzung von Betroffenenrechten weiter zu stärken.

---

[92] BVerfGE 120, 274 ff.
[93] Bundesverfassungsgericht unter dem Aktenzeichen 1 BvR 2821/16
[94] BGBl. 2016 I Nr. 8, S. 233 ff.
[95] Vgl. § 3 UKlaG
[96] Dr. Axel Halfmeier: Die neue Datenschutzverbandsklage, NJW 2016, 1126 ff.
[97] Datenschutz Praxis, September 2017, S. 6
[98] Dr. Axel Halfmeier: Die neue Datenschutzverbandsklage, NJW 2016, 1126 ff.

Die Ermöglichung von Verbandsklagen ist im Grundsatz eine sinnvolle Maßnahme für die Durchsetzung der Betroffenenrechte und die Beseitigung von Vollzugsdefiziten im Datenschutz.
Die Entwicklung in diesem Bereich bleibt spannend, da durch die „Richtlinie über Verbandsklagen zum Schutz der Kollektivinteressen der Verbraucher" das Verbandsklagerecht im Datenschutzbereich ausgeweitet werden soll. Hingegen gibt es aus Bayern Bestrebungen, das Verbandsklagerecht einzuschränken um missbräuchliche (und ggf. unionsrechtswidrige) datenschutzrechtliche Abmahnungen, die aufgrund der neuen DS-GVO allgemein befürchtet werden, einzudämmen.[99]

2.3.6 Das datenschutzrechtlichen Medienprivileg

Art. 85 DS-GVO befasst sich mit dem Spannungsverhältnis des Datenschutzes einerseits und den besonderen Anforderungen der Meinungs-, Rundfunk- und Pressefreiheit andererseits. Er trägt den Mitgliedstaaten in diesem Zusammenhang auf, durch eigene Rechtsvorschriften dieses Spannungsverhältnis aufzulösen oder doch zumindest die widerstreitenden Vorgaben in einen verträglichen Ausgleich zu bringen.[100] Hierzu räumt er den Mitgliedstaaten einen sehr weitgehenden Gestaltungsspielraum ein, der das Recht umfasst, Abweichungen von den meisten Vorgaben der DS-GVO vorzusehen und sogar die Anwendung ganzer Kapitel der DS-GVO insoweit abzubedingen.[101]

Voraussetzung ist eine Verarbeitung personenbezogener Daten zu journalistischen Zwecken[102], wobei der Begriff des Journalismus nach den Vorstellungen der Grundverordnung, wie er in deren Erwägungsgrund 153 zum Ausdruck kommt, weit ausgelegt werden soll. Diesen sehr weiten Begriff des Journalismus haben die deutschen Gesetzgeber, wenn man der gegenwärtigen Diskussion folgen möchte, nur teilweise in das Medienprivileg übernommen, wohl um die mit dem so entstehenden Medienprivileg verbundenen Freiräume insbesondere im Hinblick auf bestimmte Erscheinungsformen des Internets personell einzugrenzen.

Der deutsche Gesetzgeber hat dieses Medienprivileg in einer weitgehend gleichlautenden Form in unterschiedlichen Gesetzen niedergelegt. In einer allgemeinen Form ist es unterdessen in Art. 38 BayDSG enthalten. Für den Bereich des Rundfunks ergibt es sich seit dem 21. Rundfunkänderungsstaatsvertrag aus dem neu geschaffenen § 9c RStV, der für Telemedien durch die Neuregelung des § 57 RStV ergänzt wird.

In der bis einschließlich 24.05.2018 geltenden Rechtslage war das für den in Trägerschaft der Landeszentrale veranstalteten Rundfunk maßgebliche Medienprivileg in der jeweils

---

[99] https://www.bundesanzeiger-verlag.de/gesetze/nachrichten/detail/artikel/bayern-will-datenschutz-grundverordnung-einschraenken-26108.html, Aufruf 30.11.2018
[100] Vgl. Art. 85 Abs. 1 DS-GVO
[101] Vgl. Art. 85 Abs. 2 DS-GVO
[102] Art. 85 Abs. 2 DS-GVO nennt daneben auch wissenschaftliche, künstlerische und literarische Zwecke, die in diesem Zusammenhang jedoch von nachrangiger Bedeutung sind.

vormaligen Fassung des Art. 20 Abs. 2 BayMG und § 47 Abs. 2 RStV enthalten. Die Regelungen für die Presse wie auch die für die unterschiedlichen Anstalten des öffentlich-rechtlichen Rundfunks geltenden Bestimmungen wiesen vormals gewisse Abweichungen in der Ausgestaltung wie auch der Tragweite des Medienprivilegs auf, die nunmehr durch die weitestgehend einheitlichen Neuregelungen verschwunden sind.

Nach diesen Neuregelungen gelten von den Vorgaben der DS-GVO nurmehr die Bestimmungen der Art. 5 Abs. 1 lit. f i.V.m. Abs. 2, der Art. 24 und 32 sowie die Kap. I, VIII, X und XI. Letztere stehen nach den Vorgaben der DS-GVO auch für Zwecke des Medienprivilegs nicht zur Disposition.[103] Sogar die in der DS-GVO besonders betonten Betroffenenrechte sind demzufolge ebenso wie die Regelung der DS-GVO über die Aufsicht durch die Vorgaben des Medienprivilegs für diesen Bereich außer Kraft gesetzt. An ihrer Stelle gelten nur die jeweils für das entsprechende Medium anzuwendenden deutschen, im Fall der Landeszentrale bayerischen Vorgaben. Betroffenen Personen stehen anstelle der Rechte nach der DS-GVO nur die Rechte nach § 9c Abs. 2 und 3 RStV zu.

[103] Vgl. Art. 85 Abs. 2 DS-GVO

2.4 Bayerisches Landesrecht

2.4.1 Bayerisches Mediengesetz

Die im Berichtzeitraum vorgenommenen Änderungen im Bayerischen Mediengesetz[104] entfalteten keine datenschutzrechtlichen Wirkungen. Die durch das Inkrafttreten der DS-GVO notwendig gewordenen Anpassungen[105] wurden als Teil des Art. 39b des Gesetzes zur Änderung des Bayerischen Datenschutzgesetzes[106] vom 15.05.2018 vom Landtag beschlossen und traten am 25.05.2018 in Kraft.

2.4.2 Rundfunkstaatsvertrag

Die im Berichtzeitraum erfolgten Änderungen des Rundfunkstaatsvertrages entfalteten keine datenschutzrechtlichen Wirkungen. Mit dem 21. Rundfunkänderungsstaatsvertrag wurden zum 25.05.2018 und damit zeitgleich mit dem Inkrafttreten der DS-GVO die zur Anpassung an die durch die DS-GVO geschaffene neue Rechtslage erforderlichen Veränderungen vor allem im Hinblick auf das nunmehr anzuwendende materielle Recht und das neugefasste Medienprivileg[107] vorgenommen.

2.4.3 Rundfunkbeitragsstaatsvertrag

Hinsichtlich der Frage, ob beim Übergang von der Rundfunkgebühren- auf die Rundfunkbeitragsfinanzierung die Belange des Datenschutzes hinreichend berücksichtigt wurden, existierten nicht unerhebliche Auffassungsunterschiede. Während die Landesbeauftragten für den Datenschutz eklatante Normdefizite beklagten, waren die Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio der Auffassung, dass durch die Änderungen sogar eine Verbesserung des Datenschutzes einträte. Auch der **einmalige** Meldedatenabgleich mit ca. 70 Mio. übermittelten Datensätzen, der es anlässlich der Systemumstellung möglich machen sollte, die bisher nicht erfassten Beitragsschuldner zu ermitteln, wurde eher positiv bewertet.[108]

Mit dem 19. Rundfunkänderungsstaatsvertrags war die Vorschrift des § 11 RBeitrStV modifiziert worden. Neben dem neu eingefügten Erfordernis, dass eine vorherige Datenerhebung unmittelbar beim Betroffenen erfolglos geblieben wäre oder nicht möglich

---

[104] Gesetz zur Änderung des Bayerischen Mediengesetzes und des Gesetzes zur Ausführung des Rundfunkstaatsvertrags, des Jugendmedienschutz-Staatsvertrags, des Rundfunkbeitragsstaatsvertrags vom 12. Juli 2016 (GVBl. S. 159), Gesetz zur Änderung des Bayerischen Mediengesetzes vom 13. Dezember 2016 (GVBl. S. 350) und Gesetz zur Änderung des Bayerischen Rundfunkgesetzes und des Bayerischen Mediengesetzes vom 20. Dezember 2016 (GVBl. S. 427, ber. 2017, S. 17)
[105] Vgl. dazu unten 2.4.5
[106] GVBl. 2018, S. 230
[107] Vgl. hierzu die §§ 9c und 57 RStV-neu, sowie ausführlicher oben 2.3.6
[108] Vgl. auch die Eckpunkte von ARD, ZDF und Deutschlandradio für eine Konkretisierung der datenschutzrechtlichen Regelungen im Vollzug des 15. RÄndStV vom November 2011.

sei,[109] enthält die Norm seitdem auch eine Präzisierung, welche öffentlichen und nichtöffentlichen Stellen zur Übermittlung der Daten einzelner Inhaber von Wohnungen oder Betriebsstätten an die zuständige Landesrundfunkanstalt befugt sind. Zudem wurde ein neuer § 11 Abs. 7 eingefügt, wonach die zuständige Landesrundfunkanstalt auf das datenschutzrechtliche Auskunftsersuchen eines Beitragsschuldners diesem die Stelle mitzuteilen hat, die ihr die jeweiligen Daten des Beitragsschuldners übermittelt hat. Die Änderung trat am 01. Januar 2017 in Kraft.

2.4.4 Änderung des Bayerischen Datenschutzgesetzes (BayDSG)

Das bayerische Datenschutzgesetz wurde aufgrund des Bayerischen E-Gouvernement-Gesetzes vom 22.12.2015 (GVBl. S. 458) in mehreren Punkten[110] verändert. Die bedeutenste Veränderung bildete die Einführung des Art. 36 BayDSG, mit dem ein allgemeines Recht der Bürger auf Informationszugang gegenüber öffentlichen Stellen in Bayern eingeführt wurde (vgl. näher: 12. Tätigkeitsbericht, S 22 f.).

Anders als das Bundes-IFG bzw. die Transparenz- und Informationsfreiheitsgesetze anderer Bundesländer setzt das Auskunftsverlangen in Bayern die Glaubhaftmachung eines berechtigten, nicht auf eine entgeltliche Weiterverwendung gerichteten Interesses voraus. Die einzige im Berichtszeitraum erfolgte Änderung des BayDSG[111] erfolgte durch § 2 des Gesetzes zur effektiven Überwachung gefährlicher Personen vom 24. Juli 2017 (GVBl. S. 388), mit dem die in Art 21a Abs. 5 festgelegte Frist im Hinblick auf die Löschpflicht bei Videobeobachtung für Videoaufzeichnungen und daraus gefertigte Unterlagen von drei Wochen auf zwei Monate erweitert wurde.

2.4.5 Anpassungen des Bayerischen Rundfunk-Datenschutzsystems zum 25.05.2018

Mit dem Inkrafttreten der DS-GVO musste das bis dahin geltende rundfunkrechtliche Datenschutzsystem den nunmehr geltenden Bedingungen angepasst werden. Zu diesem Zwecke wurden im Rahmen der Neufassung des Bayerischen Datenschutzgesetzes[112] vom 15.05.2018 als Teil von dessen Art. 39b, der Änderungen zu 20 weiteren Gesetzen enthält, vom Landtag auch Anpassungen im Bayerischen Mediengesetz und Bayerischen Rundfunkgesetz vorgenommen, die am 25.05.2018 in Kraft traten.

Seither besteht beim Bayerischen Rundfunk ein Rundfunkdatenschutzbeauftragter und bei der Landeszentrale ein Medienbeauftragter für den Datenschutz (Mediendatenbeauf-

---

[109] Vgl. § 11 Abs. 4 RBeitrStV
[110] Betroffen waren die Art. 4, 15, 26, 27a und 28
[111] Mit Gesetz vom 15.05.2018 (GVBl. 2018, S. 230), in Kraft getreten am 25.05.2018 wurde das Bayerischen Datenschutzgesetzes der neuen Rechtslage nach der DS-GVO angepasst und zu diesem Zweck weitestgehend überarbeitet.
[112] GVBl. 2018, S. 230

tragter), die die jeweils zuständige Aufsichtsbehörde im Sinne des Art. 51 DS-GVO darstellen. Während sich die sachliche Zuständigkeit des Rundfunkdatenschutzbeauftragten nur auf den BR und dessen Beteiligungsunternehmen bezieht, führt der Mediendatenbeauftragte auch die Aufsicht über die Anbieter nach dem System des BayMG.

Diese Grundkonstruktion ähnelt deutlich der vormals geltenden Rechtslage und passt die Ausgestaltung den Vorgaben der DS-GVO an. Damit werden Datenschutzaufsichtsinstitutionen nach den Vorgaben der DS-GVO geschaffen, die gleichzeitig aber auch dem verfassungsrechtlichen Gebot der Staatsferne des Rundfunks nach dem Grundgesetz entsprechen.

3 Funktion des Beauftragten für den Datenschutz

Mit Art. 20 BayMG als bereichspezifischer Datenschutznorm hatte der Gesetzgeber das aus den verfassungsrechtlichen Vorgaben der Rundfunkfreiheit resultierende Gebot der Staatsferne der Landeszentrale auch für den Bereich des Datenschutzes umgesetzt. Diese gesetzgeberische Gestaltung, die einerseits der Rechtsprechung des Bundesverfassungsgerichts zum Recht auf informationelle Selbstbestimmung Rechnung trug und andererseits ausdrücklich das Medienprivileg aufnahm, hatte sich nachhaltig bewährt. Folgerichtig wurden sie mit gewissen durch die DS-GVO erforderlich gewordenen Anpassungen in das Folgesystem übernommen und dort fortgeführt.

Durch den im Berichtszeitraum noch amtierenden Beauftragten für den Datenschutz bei der Landeszentrale konnten die spezifischen Anforderungen im Bereich des in öffentlich-rechtlicher Trägerschaft betriebenen Rundfunks gewährleistet werden. Auch stellt die gewählte Gestaltung sicher, dass bei der Rechtsanwendung die spezifischen Bedingungen des Rundfunks wie auch die bestehenden verfassungsrechtlichen Besonderheiten Berücksichtigung fanden.

Durch die gewählte Gestaltung entfiel zudem die ansonsten erforderliche, im Einzelfall aber immer schwierige und auch problematische Abgrenzung zwischen Daten, die dem Medienprivileg unterfallen, und denen der Verwaltungsangelegenheiten der Landeszentrale bzw. der Anbieter, da die Aufsicht wie beim öffentlich-rechtlichen Rundfunk i.d.R. üblich in einer Hand zusammengefasst ist. Der Beauftragte für den Datenschutz bei der Landeszentrale überwachte gem. Art. 20 Abs. 3 S. 2 BayMG (alt) die Einhaltung der Vorschriften des BayMG sowie anderer Vorschriften über den Datenschutz bei der Landeszentrale und bei den Anbietern umfassend,[113] und zwar auch, soweit es sich um Verwaltungsangelegenheiten handelt.[114] Mit dieser umfassenden Zuständigkeit für alle Aufgaben bei der Landeszentrale und den Anbietern trug das BayMG den verfassungsrechtlichen Anforderungen an einen rundfunkrechtlichen Datenschutz Rechnung.[115]

Weitere Aufgaben des Beauftragten für den Datenschutz waren die Beratung bei datenschutzrechtlichen Fragen, die Mitarbeiterschulung in der Landeszentrale und die Beratung von Anbietern bei datenschutzrechtlichen Problemen.

---

[113] Zur Frage der inhaltlichen Reichweite dieser Aufgabe vgl. *Gummer,* Fragen des Datenschutzes bei neuen Formen von Programmen und Mediendiensten, ZUM 2004, 546. Zudem sind seit dem Inkrafttreten des 9. Rundfunkänderungsstaatsvertrages auch dessen Regelungen zur Datenschutzaufsicht über Telemedien und die Datenschutzaufsicht beim öffentlich-rechtlichen Rundfunk von Bedeutung.

[114] Vgl. Art. 20 Abs. 3 S. 3 BayMG (alt).

[115] Zu dieser Thematik hat der Norddeutsche Rundfunk ein sehr instruktives Gutachten bei Prof. Dr. Dieter Dörr erstellen lassen und 2002 als Band 13 der „Studien zum deutschen und europäischen Medienrecht" veröffentlicht. Es trägt den Titel: „Rundfunk und Datenschutz - Die Stellung des Datenschutzbeauftragten des Norddeutschen Rundfunks."

Der Beauftragte hatte bei der Durchführung seiner Aufgaben Auskunfts-, Kontroll-, Zugriffs-, Einsichts- und Beanstandungsrechte.[116] Der Beauftragte für den Datenschutz bei der Landeszentrale war aber auch bereits in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Die Stellung des Beauftragten entsprach damit auch bereits in der vormaligen, bis einschließlich 24.05.2018 geltenden Ausgestaltung der des Bayerischen Landesbeauftragten für Datenschutz bzw. des Präsidenten des Landesamtes für Datenschutzaufsicht und entsprach somit auch zweifelsfrei den Anforderungen des Europarechts[117] einschließlich der EU-Datenschutzrichtlinie,[118] die in Art. 28 Abs. 1 den Mitgliedstaaten auferlegt, datenschutzrechtliche Kontrollstellen zu schaffen, die die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahrnehmen.

Der Beauftragte für den Datenschutz bei der Landeszentrale unterstand nach Art. 20 Abs. 3 S. 7 BayMG (alt) intern der Dienstaufsicht des Verwaltungsrates. Zur Dienstaufsicht waren nur arbeitsrechtliche Belange zu zählen. Eine Delegation der Dienstaufsicht an andere Organe der Landeszentrale oder leitende Angestellte war nicht möglich.

Insbesondere bestand keine Einordnung des Beauftragten für den Datenschutz bei der Landeszentrale in den durch den Präsidenten der Landeszentrale geleiteten Verwaltungsaufbau. Der Präsident berief zwar den Beauftragten für den Datenschutz bei der Landeszentrale, bedurfte hierfür aber der Zustimmung des Verwaltungsrates.[119]

Im Übrigen bestanden für den Präsidenten oder für von diesem beauftragte Personen keine Aufsichtsbefugnisse über oder sonstige Beeinflussungsmöglichkeiten hinsichtlich des Beauftragten für den Datenschutz bei der Landeszentrale. Vielmehr führt dieser in datenschutzrechtlicher Hinsicht die Aufsicht über die Landeszentrale und ihren Verwaltungsaufbau. Er war dennoch Teil der Landeszentrale und Ausdruck ihrer staatsfernen Selbstverwaltung, was die interne Dienstaufsicht durch den Verwaltungsrat unterstrich.

Mit der DS-GVO, die die europarechtlich erforderliche Unabhängigkeit noch etwas stärker akzentuiert, haben sich die Gewichte nochmals etwas verschoben, so dass ab dem neuen Berichtszeitraum nunmehr neben der Ausfüllung der Stellung des Mediendatenbeauftragten keine anderen Aufgaben innerhalb der Landeszentrale mehr übernommen werden dürfen.

---

[116] Vgl. insbes. Art. 20 Abs. 4 BayMG (alt).
[117] Art. 8 Abs. 3 EU-Grundrechtecharta wie auch Art. 16 Abs. 2 AEUV sehen eine Beaufsichtigung durch unabhängige Stellen zwingend vor.
[118] RL 95/46/EG, ABl. EG vom 23.11.1995, Nr. L 281/31.
[119] Vgl. Art. 20 Abs. 3 S. 1 BayMG (alt).

4 Datenschutz in der Landeszentrale

4.1 Allgemeines

Mit der Geschäftsleitung fand im Berichtszeitraum regelmäßig, i.d.R. vierteljährlich ein Informationsaustausch statt, in dessen Rahmen allgemeine, den Datenschutz in der Landeszentrale betreffende Fragen erörtert wurden.

Gelegentlich waren auch speziellere Fragen aus dem Bereich des Datenschutzes Gegenstand von Anfragen und Ausarbeitungen, die auch über den unmittelbaren Zuständigkeitsbereich der Landeszentrale hinausgehen konnten.

Zur Informationstätigkeit gehörten zudem die Unterrichtung von Gremien und Organen der Landeszentrale über grundsätzlichere oder auch speziellere Fragen des Datenschutzes und Vorträge im Rahmen von Veranstaltungen der Landeszentrale.

Im Rahmen einer Fortbildungsreihe der Landeszentrale für Mitarbeiter wurde im Jahr 2016 eine Veranstaltung mit dem Titel „Datenschutz und HbbTV" gestaltet. Hierbei wurden die Mitarbeiter nicht nur über die Grundzüge des Datenschutzes informiert, sondern auch vor dem Hintergrund der Entwicklung von der linearen Übertragung hin zu den Anwendungen der digitalen TV-Welt die Auswirkungen auf den Datenschutz und die Gestaltung der Rundfunkangebote näher erläutert.

Im Februar 2018 wurde in einer weiteren Veranstaltung in dieser Reihe ein Vortrag über das neue europäische Datenschutzrecht angeboten, das mit dem Inkrafttreten der Datenschutz-Grundverordnung ab dem 25.05.2018 in Europa zu beachten sein würde. In diesem Zusammenhang wurde ein Bogen von den historischen Hintergründen und den mit der Grundverordnung verfolgten Zielsetzungen, über die Grundzüge des neuen Datenschutzrechtes bis hin zu den Auswirkungen für die Landeszentrale geschlagen.

Im März 2018 folgte eine zweiteilige Informationsveranstaltung für Anbieter der Landeszentrale. Diese befasste sich ausgehend von den eben geschilderten Erwägungen und daran angelehnten Erläuterungen mit den maßgeblichen Folgewirkungen der eintretenden Rechtsänderung für Rundfunkanbieter und einem Bündel von ausgewählten Fragestellungen, die auf einer Abfrage von Anbieterverbänden beruhten.

Anfang Mai 2018 beteiligte sich der Datenschutz der Landeszentrale an einem Workshop des Instituts für europäisches Medienrecht (EMR) und der Arbeitsgemeinschaft privater Rundfunk (APR) zum Themenkreis „Datenschutz und Datensicherheit" in Frankfurt mit einem eigenen Vortrag zum Thema „Datenschutz für Medienunternehmen nach dem 21. Rundfunkänderungsstaatsvertrag". Dieser befasste sich vor allem mit dem im Hinblick

auf die Datenschutz-Grundverordnung neu gefassten Medienprivileg, seinen Voraussetzungen, seiner Ausgestaltung und seinen Folgewirkungen.

Auf europäischer Ebene wirkte der Datenschutz der Landeszentrale zuvor bereits an dem Workshop „The grey areas between media regulation and data protection" mit. Der englischsprachige Workshop wurde vom „European Audiovisual Observatory" in Straßburg organisiert. Hierbei konnte im Rahmen der Diskussion in einer Zusammenfassung der Sicht der Datenschutzregulierer, der Datenschützer, der Nutzer und der Industrie die Sicht des Datenschutzes im Bereich privater Rundfunkanbieter mit einfließen. Die Erwartungen der Workshopteilnehmer an die EU-Kommission konnten zusammengefasst und an diese weitergeleitet werden.

Seit 2017 nimmt der Bereich Datenschutz der Landeszentrale an dem Arbeitskreis Arbeitshilfen des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V. teil und unterstützt diesen aktiv bei der Erstellung von Arbeitshilfen. Im Jahr 2017 wurde ein Schulungskonzept erstellt und im Anschluss daran mit der Ausarbeitung eines Kurzaudits begonnen.

Von besonderer Bedeutung für die Arbeit des Datenschutzes der Landeszentrale war, wie auch bereits in den Vorjahren, der regelmäßige Austausch mit dem Landesamt für Datenschutzaufsicht in Bayern und die Teilnahme an dem Arbeitskreis Medien des Düsseldorfer Kreises bzw. der Datenschutz-Konferenz (DSK).

4.1.1 Datenschutzrechtliche Freigabe automatisierter Verfahren nach Art. 26 BayDSG (alt)

Die Landeszentrale ist gem. Art. 26 Abs. 1 BayDSG (alt) verpflichtet, den erstmaligen Einsatz von bestimmten automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden bzw. wesentliche Veränderungen solcher Verfahren datenschutzrechtlich freizugeben. Die datenschutzrechtliche Freigabe verfolgt den Zweck, Verletzungen der Datenschutzvorschriften von vornherein zu vermeiden.

Im Berichtszeitraum waren dem Datenschutz in der Landeszentrale zwei neue automatisierte Verfahren vorgelegt worden.
Dabei ging es einerseits um ein Workflow-Programm, mit welchem die Arbeitsprozesse in der Landeszentrale im Rahmen von Programmänderungen abgebildet und ab der Antragstellung vollständig digitalisiert werden sollten. Aus datenschutzrechtlicher Hinsicht kam es bei der datenschutzrechtlichen Prüfung vor allem darauf an, die in diesem Zusammenhang erfassten personenbezogenen Daten sowie den Zugang zu diesen auf das sich aus Aufgaben der Landeszentrale ergebende dienstlich Notwendige zu beschränken. Auf der Basis in diesem Zusammenhang getroffener Vereinbarungen konnte das fragliche Verfahren in seinem seinerzeitigen Entwicklungsstand zur Erprobung und zur Gewinnung praktischer Erfahrungen und genauerer Erkenntnisse über die in diesem Zusammenhang bestehenden dienstlichen Bedürfnisse einstweilig freigegeben werden.

Andererseits war die Einführung eines Programms Ende 2017 auf den Weg gebracht worden, über welches zahlreiche Fragen von der Arbeitszeiterfassung über die Gewährung von Urlaub und Freistellung von der Arbeitszeit bis zu Gesichtspunkten der Zutrittskontrolle erfasst und verarbeitet werden sollten. Wegen der Komplexität des Prozesses war es nicht möglich gewesen, die datenschutzrechtliche Prüfung bis zum Übergang des materiellen Rechtes auf die neue Basis nach der DS-GVO zu einem Abschluss zu bringen.

Der Beauftragte bemühte sich zudem weiterhin um eine Bestandserhebung aller tatsächlich eingesetzten automatisierten Verfahren, auch der nicht freigabepflichtigen, in deren Zuge personenbezogene Daten verarbeitet werden.

4.1.2 Verfahrensverzeichnis nach Art. 27 BayDSG (alt)

Die Landeszentrale führt gem. Art. 27 BayDSG (alt) ein Verzeichnis der bei ihr eingesetzten und datenschutzrechtlich freigegebenen automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden. Dieses Verfahrensverzeichnis wird jährlich fortgeschrieben. In diesem Verzeichnis sind für jedes automatisierte Verfahren die in Art. 26 Abs. 2 BayDSG (alt) genannten Angaben festzuhalten:

1. Bezeichnung des Verfahrens,
2. Zweck und Rechtsgrundlage der Erhebung, Verarbeitung oder Nutzung,
3. Art der gespeicherten Daten,
4. Kreis der Betroffenen,
5. Art der regelmäßig zu übermittelnden Daten an den Empfänger,
6. Regelfristen für die Löschung der Daten oder für die Prüfung der Löschung,
7. verarbeitungs- und nutzungsberechtigte Personengruppen,
8. im Fall der Auftragsdatenverarbeitung, Art. 6 Abs. 1-3 BayDSG, die Auftragnehmer,
9. Empfänger vorgesehener Datenübermittlungen in Drittländer.

Auch wenn die vormals bestehende Pflicht zur Führung eines Anlageverzeichnisses weggefallen ist, ist mit der IT-Abteilung vereinbart, dass dieses Anlageverzeichnis in gewisser Weise fortgeführt wird. Ein Verwaltungsaufwand entsteht hierdurch nicht, da die eingesetzte Hardware sowie die Peripherie-Geräte weiter inventarisiert und als Anlagevermögen aktiviert und daher im Anlagespiegel geführt werden. Der Anlagespiegel unterstützt insoweit auch Planungen bei der Entwicklung von Konzepten auf dem Gebiet der Datensicherheit.

4.2 Verwaltungsgebäude der Landeszentrale

Das schon vor Beginn des letzten Berichtszeitraums erreichte hohe Sicherheitsniveau konnte erhalten werden. Der Umgang mit zahlreichen, teilweise auch externen Veranstaltungen hat sich unterdessen gut eingespielt. Die in früheren Jahren bestehenden offenen Fragen auf dem Gebiet der Datensicherheit, im Zusammenhang mit der Reinigung der Büroräume und insbesondere dem unbefugten Zutritt Dritter zu nicht-öffentlichen Bereichen der Landeszentrale bzw. zu sensiblen Bereichen der Datenverarbeitungsanlagen, können seit längerem als gelöst angesehen werden.

Nennenswerte Auffälligkeiten konnten im Berichtszeitraum nicht festgestellt werden

4.3 **Fragen in Bezug auf Datenverarbeitungsprozesse in der Landeszentrale**

Im Berichtszeitraum wurden die Mitarbeiter, in deren Aufgabenbereich personenbezogene Daten erhoben, verarbeitet und genutzt werden, gezielt im Hinblick auf die sich stellenden Fragen beraten. Hierbei hat sich gezeigt, dass die Mitarbeiter der Landeszentrale gerade bei Fragen des Datenschutzes in einem hohen Maße sensibilisiert sind. Bei Zweifelsfragen wenden sie sich in der Regel selbstständig und umgehend an den Beauftragten für den Datenschutz.

Dies gilt auch für Fragen, die die Datensicherheit und die Integrität von Verarbeitungsprozessen betreffen. Sowohl die Gestaltung der Systeme wie auch der Umgang mit problematisch erscheinenden Vorgängen wird laufend und insbesondere auch in auftretenden Einzelfällen in Abstimmung mit dem Beauftragten gestaltet und fortentwickelt.

Im Berichtszeitraum ergaben sich Aufgaben und Anfragen an den Beauftragten für den Datenschutz aus nahezu allen Bereichen. Insgesamt war festzustellen, dass sich in den aufgetretenen Fragestellungen die mit der fortschreitenden Digitalisierung aller Arbeitsprozesse wachsenden Anforderungen widerspiegeln. Soweit die angesprochenen Themen von allgemeinem Interesse sind, werden diese im Folgenden dargestellt.

4.3.1 **Zulässige Nutzung vorhandener Daten**

Den Ausgangspunkt bildet im öffentlichen Bereich stets die in zahlreichen Normen niedergelegte Berechtigung, diejenigen personenbezogenen Daten zu erheben, zu spei-

chern, zu verändern oder zu nutzen, die zur Erfüllung der in die Zuständigkeit der entsprechenden Stelle fallenden Aufgaben erforderlich sind.[120]

Daraus ergeben sich immer wieder und in unterschiedlichen Gestaltungen Fragen, in welchen Zusammenhängen bei der Landeszentrale vorhandene bzw. für bestimmte Zielsetzungen erhobene Daten konkret genutzt werden dürfen.

Für die Beantwortung dieser Frage ist in aller Regel zunächst der Lebenssachverhalt und Sachzusammenhang zu ermitteln, in dem die Daten der Landeszentrale zugänglich wurden. Aus diesen lassen sich sodann die der Landeszentrale zustehenden Berechtigungen und insbesondere auch die jeweils anzunehmende Tragweite einer ausdrücklich erteilten bzw. sich konkludent ergebenden Einwilligung ermitteln.

Unter Berücksichtigung der auf der Seite des jeweiligen Betroffenen bestehenden schutzwerten Interessen können sodann Hinweise und Empfehlungen für den Umgang mit den fraglichen Daten im Einzelfall entwickelt werden.

Besondere Aktualität erlangten diese Fragen durch den Wechsel des geltenden materiellen Rechtes hin zur DS-GVO, weil häufig zweifelhaft erschien, ob und wenn ja unter welchen Voraussetzungen in der Vergangenheit angefallene und nunmehr vorhandene Daten auch unter Geltung des neuen Rechtes weiterhin genutzt werden könnten. Bedeutsam erschien es daher in diesen Fällen zu ermitteln, in welchem Zusammenhang die Daten jeweils erhoben worden waren und welche Rechtfertigungen für die Landeszentrale hierfür bestanden. Hierbei war insbesondere zu berücksichtigen, dass auch in der Vergangenheit wirksam erteilte Einwilligungen unter Geltung des neuen Rechtes prinzipiell ihre Bedeutung behalten können und daher gerade keine flächendeckende Einholung nochmaliger Einwilligungen generell erforderlich wurde. Dennoch waren mit der Annäherung an den 25.05.2018 stetig häufiger werdende Anfragen zu prüfen und zu beantworten.

4.3.2 Zulässige Zweckänderung

Im Zusammenhang damit ergibt sich häufig die weitere Frage, ob und wenn ja zu welchen ggf. auch weiteren Zwecken die Daten genutzt werden dürfen, die die Landeszentrale zumeist auf ganz unterschiedliche Weise und in unterschiedlichen Zusammenhängen erhalten hat.

Aus diesen Umständen ergibt sich in aller Regel eine konkrete Zweckbindung, die die weiteren Möglichkeiten des Einsatzes dieser Daten und der sich daraus ergebenden Erkenntnisse beschränkt. Dieser Grundsatz der Zweckbindung gehört zu den grundlegen-

---

[120] Vgl. z.B. Art. 16 Abs. 1 und Art. 17 Abs. 1 Nr. 1 BayDSG (alt).

den Erkenntnissen deutschen Datenschutzrechtes[121] und behält auch seine Gültigkeit im Rahmen der Anwendung der DS-GVO, vgl. Art. 5 Abs. 1 lit. b.

Aus diesem Grunde ist die Ermittlung des ursprünglichen Nutzungszweckes von besonderer Bedeutung, so dass derartige Nachfragen stets eine hohe Berechtigung besitzen. Andererseits erlaubte das für die Landeszentrale maßgebliche BayDSG zahlreiche Nutzungsänderungen,[122] deren Tatbestandsvoraussetzungen im Einzelfall zu prüfen waren. Insbesondere bei Daten, die für Aufsichts- und Kontrollbefugnisse der Landeszentrale erforderlich sind, waren in der Regel auch Nutzungsänderungen wenn auch mit einer entsprechenden Beschränkung zulässig.[123] Gleichwohl musste hierfür eine Einwilligung, das offensichtliche Interesse des Betroffenen oder eine gesetzliche Ermächtigungsnorm vorliegen, deren Voraussetzungen im konkreten Einzelfall jeweils überprüft werden musste. Unter Geltung des neuen Rechtes ergeben sich insoweit gewisse Veränderungen im Prüfungsmaßstab.

4.3.3 Übermittlung von personenbezogenen Daten an Dritte

Immer wieder wird die Frage gestellt, welche Daten an Dritte übermittelt werden dürfen. Der Standpunkt des Gesetzes wie auch der Landeszentrale hierzu ist sehr klar. Personenbezogenen Daten sind zu schützen; um solche handelt es sich nur bei Daten, die sich auf natürliche Personen beziehen, nicht hingegen bei Daten einer juristischen Person.

Während im vorherigen Berichtszeitraum mehr Fragen zur Übermittlung von Anbieterdaten insbesondere an Dritte im Brennpunkt standen, waren im gegenwärtigen Berichtszeitraum eher Fragen nach der Weitergabe von Mitarbeiterdaten der Landeszentrale zur vermeintlich einfacheren Erreichbarkeit der Landeszentrale bzw. einzelner Sachgebiete von Interesse.
Es war z.B. zu überprüfen, ob ggf. das Recht auf Auskunft[124] über den Inhalt von Dateien und Akten öffentlicher Stellen die Weitergabe von Listen mit Vornamen, Nachnamen, Bereichszugehörigkeit, Telefon- und Telefaxnummer rechtfertigen kann. Ggf. können dem Begehren und dem Auskunftsanspruch jedoch öffentliche Interessen entgegenstehen.[125] Das Bundesverwaltungsgericht hat in einem nahezu gleichgelagerten Fall die Ansicht vertreten, dass derartige Maßnahmen die effektive Aufgabenerledigung stören und die Arbeit der Bediensteten beeinträchtigen könnten.[126] In der Gesamtbetrachtung spräche jedoch nichts dagegen, spezielle Funktionsadressen einzurichten, um eine gute Erreichbarkeit zu gewährleisten.

---

[121] Vgl. bereits das sog. Volkszählungsurteil des BVerfG vom 15.12.1983 (BVerfGE 65, 1 ff.).
[122] Vgl. insbesondere Art. 17 Abs. 2 BayDSG (alt).
[123] Vgl. Art. 17 Abs. 3 S. 1 BayDSG (alt).
[124] Art. 36 BayDSG (alt).
[125] Art. 36 Abs. 1 S. 2 Nr. 1 BayDSG (alt).
[126] BVerwG, Urteil vom 20.10.2016, 7 C 20.15 in NJW 2017, 1258 ff.

Ein weiterer Fragenkomplex betraf die Rechtmäßigkeit der Veröffentlichung von Teilnehmerdaten in Form einer Liste sowie die Bekanntgabe der Veranstaltungsteilnehmer im Internet im Rahmen des konkreten Veranstaltungsangebotes. Da es sich auch hier um die Weitergabe personenbezogener Daten handelt, war für eine rechtmäßige Veröffentlichung der betroffenen personenbezogenen Daten entweder eine vertragliche Grundlage oder eine Einwilligung der Teilnehmer erforderlich. In diesem Zusammenhang wurden z.B. Teilnahmebedingungen entsprechend angepasst. Für Anmeldungen via Online-Formular wurde eine datenschutzfreundliche Voreinstellung geschaffen. Mittels eines Opt-in-Kästchen stand dem Interessenten bei der Anmeldung nun frei, ob seine Anmeldung für andere Event-Besucher auf der Internetseite sichtbar sein würde oder nicht.

4.3.4 Löschung von Datenträgern

Neben der laufend auftretenden datenschutzkonformen Entsorgung von Alt-Akten ergaben sich im Bereichtszeitraum neuerliche Fragen im Zusammenhang mit dem Austausch von elektronischen Bürogeräten, auf welchen aus ihrer jeweiligen Einsatzbestimmung in der Landeszentrale personenbezogene Daten gespeichert waren bzw. dieses nicht auszuschließen war. Neben der physischen Vernichtung von entsprechenden Datenträgern kommt bei technischen Geräten auch eine entsprechend sorgfältig durchgeführte Löschung sämtlicher Speicher der auszutauschen Geräte in Betracht, so dass gegebenenfalls diese Geräte auch zulässigerweise einer anderen Verwendung in einem neuen Sachzusammenhang zugeführt werden können. Gegebenenfalls ist in solchen Fällen auf ein tatsächlich wirksames Überschreiben entsprechender Speicher zu achten.

5 Datenschutzrechtliche Fragestellungen bei den Anbietern und Tochtergesellschaften der Landeszentrale

5.1 Allgemeines

Einen maßgeblichen Teil der Tätigkeit des Beauftragten für den Datenschutz bei der Landeszentrale bildete im Berichtszeitraum, wie auch in den Jahren zuvor, die Beratung der Anbieter in datenschutzrechtlichen Fragestellungen. Dabei lag der Schwerpunkt bei der rechtskonformen Ausgestaltung interner und externer Prozesse gemäß den gesetzlichen Vorgaben. In diesem Kontext waren zum einen die Bewältigung von Datenlecks sowie zum anderen der Umgang mit personenbezogenen Daten für Werbezwecke von besonderer Bedeutung.
Ein großer Anteil der eingegangenen Anfragen und Beschwerden bezog sich weiterhin auf unerwünschte oder jedenfalls nicht erbetene Werbung per Post, E-Mail oder Telefon. Die Beschwerdeanzahl hat im Berichtszeitraum nochmals zugenommen, was eine erhebliche strukturelle Herausforderung für die Bearbeitung darstellt.
Die Beschwerdeführer bemängelten nicht nur, dass sie Werbung – im Berichtszeitraum vornehmlich per E-Mail – unerwünscht erhalten hätten, sondern begehrten darüber hinaus weiterhin auch häufig Auskunft über die Herkunft ihrer personenbezogenen Daten Daten bei den Anbietern und deren Verwendungszweck. Zudem wurde zumeist auch eine Löschung oder Sperrung der Daten und eine Bestätigung dieser Vorgänge gefordert, eine Untersagung der zukünftigen Speicherung ohne Genehmigung wie auch der Übermittlung an Dritte bzw. die Löschung aller gespeicherten Daten beantragt.
Hier war auffällig, dass sich ein erheblicher Anteil der Beschwerdeführer darüber beklagte, dass ihre Auskunftsersuchen vom jeweiligen Anbieter nicht oder nicht ausreichend beantwortet wurden.

Auch das Thema Werbung trotz eines bereits ausgesprochenen Werbewiderrufs war wieder verstärkt Gegenstand von Beschwerden.
Bei der Prüfung fiel jedoch auf, dass in etlichen Fällen ein Widerruf nicht für alle zuvor vom Nutzer bzw. Kunden freigebebenen Kommunikationswege erfolgt war, so dass in diesen Fällen dahingehend kein Verstoß des Anbieters vorlag. Es kam aber auch vor, dass Widersprüche in elektronische Kundenverwaltungssysteme nicht richtig eingepflegt oder den falschen Personen zugeordnet wurden. Hier mussten die Prozesse der jeweiligen Unternehmen angepasst werden, wobei der Beauftragte für den Datenschutz bei der Landeszentrale hier vor allem beratend unterstützte.[127]

In den meisten Fällen waren die Beschwerdeführer zunächst direkt an die jeweils betroffenen Anbieter herangetreten. Häufig konnten die Beschwerdeführer ihre in der Regel

[127] § 38 Abs. 1 S. 2 BDSG (alt) weist den Aufsichtsbehörden das Beraten und Unterstützen insoweit als originäre Aufgabe zu.

berechtigten Anliegen aber nicht bzw. nicht in einer ihnen akzeptabel erscheinenden Zeitspanne durchsetzen oder waren der Meinung, dass sie hierzu nach den bisherigen Erfahrungen nicht ohne Einschaltung des Beauftragten für den Datenschutz bei der Landeszentrale in der Lage wären, zu ihrem Recht zu kommen, so dass sie sich zur Einschaltung des Beauftragten veranlasst sahen.

Neben den geschilderten Fällen unzulässiger Datennutzungen für Werbezwecke oder unbeantworteter bzw. verzögerter Auskunftsersuchen erstreckten sich die Beschwerden auf zahlreiche andere Fragestellungen, wie beispielsweise die Weitergabe von Daten an Dritte. Eine besondere Herausforderung stellte dabei die datenschutzrechtliche Beurteilung von Datenweitergaben an Inkassobüros bzw. Anfragen bei Auskunfteien oder die Meldung an solche dar.

In der Regel konnte den Beschwerderführern in einem überschaubaren Zeitraum abgeholfen und die begehrte Löschung oder Sperrung von Daten bewirkt bzw. die gewünschte Auskunft oder Bestätigung über das Bestehen oder Nichtbestehen eines Rechtsverhältnisses herbeigeführt werden. Darüber hinaus liefern aber Bürgeranfragen und Beschwerden auch wertvolle Einblicke und Hinweise, die bei der Erfüllung der Aufgabe des Beauftragten für den Datenschutz bei der Landeszentrale, für die tatsächliche Einhaltung der gesetzlichen Rahmenbedingungen zu sorgen, häufig von großem Nutzen sind.

5.1.1 Datenerhebung

Bei der Erhebung von personenbezogenen Daten ist von den Anbietern gem. § 4 Abs. 3 BDSG (alt) und § 13 Abs. 1 TMG darauf zu achten, dass die Betroffenen über den Zweck, die mögliche Weitergaben an Dritte und die verantwortliche Stelle aufgeklärt werden.

5.1.2 Auftragsdatenverarbeitung

Der Trend, datenverarbeitende Tätigkeiten an andere Unternehmen auszulagern, macht auch vor Rundfunkanbietern nicht halt. Bei der Auftragsdatenverarbeitung im Sinne des § 11 BDSG (alt) werden durch andere Stellen personenbezogene Daten entsprechend eines konkreten Auftrags erhoben, verarbeitet und genutzt. Auftragsdatenverarbeiter sind im Verhältnis zu der verantwortlichen Stelle nicht als Dritte im Sinne des § 3 Abs. 8 S. 2 BDSG (alt) zu werten, soweit die Verarbeitung im Inland, innerhalb der EU oder einem anderen Staat des Europäischen Wirtschaftsraumes stattfindet. Damit ist die Datenverarbeitung als interner Vorgang der verantwortlichen Stellen zu betrachten und es findet auch keine Datenübermittlung nach § 3 Abs. 4 Nr. 3 BDSG (alt) an Dritte statt. Es gelten somit in diesem Fall die gleichen Anforderungen, wie sie für die interne Datenverarbeitung gelten, sofern die in § 11 BDSG (alt) aufgeführten Rahmenbedingungen erfüllt sind. Diese müssen explizit und konkret in einem ensprechenden Vertrag schriftlich festgelegt werden.

Sollten diese Bedingungen nicht erfüllt sein und keine Auftragsdatenverarbeitung vorliegen, ist die Zulässigkeit der Datenübertragung nach § 4 Abs. 1 und §§ 24 bis 32 BDSG (alt) zu prüfen.

5.1.2.1 Google Analytics

Wird von Anbietern im Rahmen des Webauftritts ein Webanalysedienst verwendet, ist i.d.R. ein Auftragsdatenverarbeitungsvertrag erforderlich. Sollte ein Dienst aus dem US-amerikanischen Markt wie beispielsweise Google Analytics genutzt werden und in diesem Zusammenhang personenbezogene Daten in die USA übermittelt werden, ist darauf zu achten, dass der Diensteanbieter gemäß Privacy Shield zertifiziert ist und die Zertifizierung den jeweiligen Daten entspricht. Die näheren Umstände können einer Website des US-amerikanischen Handelsministeriums entnommen werden.
Unter der Voraussetzung, dass das Privacy-Shild-Abkommen weiterhin Bestand hat, kann die Datenübermittlung dann auf die jeweilige Zertifizierung gestützt werden.

Ausblick:
Am 05.06.2018 hat das EU-Parlament für eine Aussetzung des Privacy-Shield-Abkommens votiert, da das Abkommen aus Sicht des Parlaments kein angemessenes Schutzniveau biete. Die Entscheidung des Parlaments ist für die EU-Kommission nicht bindend. Es erscheint aber unwahrscheinlich, dass sich die EU-Kommission der Forderung nach Nachbesserungen letztlich entziehen wird.
Auch dem EuGH liegen Fragen zur Wirksamkeit des Privacy-Shield-Abkommens vor. Die Vorgängerregelung, das Safe-Harbour-Abkommen, wurde durch den EuGH für ungültig erklärt.[128]

5.1.2.2 Cloud computing

Ein weiterer Aspekt der Auftragsdatenverarbeitung, der allerdings oftmals zu wenig beachtet wird, ist das sogenannte „Cloud Computing". Auch hier gelten die oben ausgeführten Empfehlungen zur Auftragsdatenverarbeitung. Bei den unter dem Schlagwort Cloud-Computing zusammengefassten Dienstleistungen werden oftmals personenbezogene Daten auf Servern externer Dienstleister verarbeitet. In den meisten Fällen handelt es sich bei den Diensteanbietern um US-amerikanische Unternehmen, deren Server in der Regel außerhalb Deutschlands bzw. außerhalb der Europäischen Union stehen.
Dabei lässt sich feststellen, dass gegenüber der datenschutzrechtlichen Problematik, die mit der Nutzung dieser Dienste einher geht, in etlichen Fällen nur eine geringe Sensibilität besteht. Generell sind auch bei der Verarbeitung personenbezogener Daten mit Hilfe von Cloud-Diensten sämtliche datenschutzrechtlichen Vorgaben einzuhalten. Dabei tritt eine Besonderheit zu Tage: Cloud-Dienste haben oftmals die Möglichkeit, ihnen übergebene Daten mit selbst erhobenen Daten oder Daten aus anderen Quellen anzureichern bzw. abzugleichen. Dadurch haben diese Diensteanbieter die Möglichkeit, vermeintlich pseudonymisierte Daten reidentifizierbar zu machen. Es ist beispielsweise keine ausrei-

---

[128] Vgl. oben 2.1.2.2

chende Pseudonymisierung, lediglich Hashwerte anstelle von E-Mailadressen zu übertragen, wenn der Dienstleister diese Hashwerte aufgrund eigener Daten wieder E-Mailadressen zuordnen kann.

5.1.3 Der betriebliche Datenschutzbeauftragte

Gemäß § 4f BDSG (alt) sind Medienanbieter, wie andere Unternehmen auch, verpflichtet, einen Datenschutzbeauftragten zu bestellen, sofern in der Regel mindestens zehn Mitarbeiter ständig mit der automatisierten Verarbeitung personenbezogener Daten oder in der Regel mindestens 20 Mitarbeiter damit beschäftigt sind, diese Daten auf andere Weise zu erheben, zu verarbeiten oder zu nutzen. Dabei ist jedoch nicht eine gelegentliche Beschäftigung gemeint, sondern vielmehr ein Schwerpunkt der jeweiligen Tätigkeit. Unter automatisierter Verarbeitung kann bereits die Nutzung von E-Mail-Diensten verstanden werden.
Für kleinere Unternehmen bzw. Anbieter besteht daher oftmals keine Pflicht einen Datenschutzbeauftragten zu benennen. Bei den meisten Anbietern wird aber mit hoher Wahrscheinlichkeit von einer Pflicht, einen Datenschutzbeauftragten zu bestellen, auszugehen sein.
Bei der Bestellung ist sicherzustellen, dass bei einem betrieblichen Datenschutzbeauftragten keine Interessenkonflikte entstehen und dass er bei der Erfüllung seiner Aufgaben nicht weisungsgebunden ist. Diese Vorgaben führen dazu, dass die Tätigkeit des Datenschutzbeauftragten mit verschiedenen anderen Aufgaben nicht vereinbar ist. Der Datenschutzbeauftragte hat die Aufgabe, Funktionsträger im Unternehmen zu beraten und zu kontrollieren. Eben diese Funktionen darf der Datenschutzbeauftragte nicht selbst bekleiden, da dies einer wirksamen Kontrollfunktion widerspricht.
Im Berichtszeitraum wurden etliche Fragen zum Themenkomplex betrieblicher Datenschutzbeauftragter von Anbietern an den Beauftragten für den Datenschutz bei der Landeszentrale herangetragen. Diese wurden erörtert und im Austausch mit den Anbietern jeweils eine entsprechende Lösung erarbeitet.

Ausblick:
Auch nach dem Inkrafttreten der DS-GVO treten keine substanziellen Änderungen hinsichtlich Aufgaben, Rechten und Pflichten des betrieblichen Datenschutzbeauftragten ein.

5.1.4 Auskunftsanspruch

Ein großer Teil der im Berichtszeitraum bearbeiteten Beschwerden befasste sich mit der in § 34 Abs. 1 BDSG (alt) festgelegten Verpflichtung, Betroffenen auf Verlangen Auskunft über die zu ihrer Person gespeicherten Daten zu erteilen. Es gab zahlreiche Fälle, in denen Anbieter dieser Verpflichtung nicht oder nicht in ausreichendem Umfang nachgekommen sind. § 34 Abs. 1 BDSG (alt) sieht vor, dass dem Betroffenen mitzuteilen ist, welche Daten über ihn gespeichert sind, woher diese Daten stammen, wem sie zugänglich gemacht wurden und zu welchem Zweck die Speicherung erfolgt. Bei den im Be-

richtszeitraum aufgetretenen Fällen wurden die jeweiligen Unternehmen aufgefordert, ihren Pflichten nachzukommen. In allen Fällen wurde der Rechtsanspruch der Betroffenen auf Auskunft im Anschluss erfüllt.

Ausblick:
Das insbesondere in Art. 15 DS-GVO festgeschriebene Auskunftsrecht bildet auch in Zukunft ein zentrales Betroffenenrecht. Da die DS-GVO aber ein erheblich schärferes Sanktionssystem vorsieht und in Art. 12 DS-GVO auch strenge Zeitvorgaben zur Erfüllung der Betroffenenrechte enthalten sind, erscheint es ratsam, der Erfüllung von Auskunftsansprüchen künftig eine besondere Aufmerksamkeit zu widmen und bei prozessualen Defiziten entsprechende Anpassungen vorzunehmen.

5.1.5 Sperrung / Löschung personenbezogener Daten

Im Zusammenhang mit Auskunftsansprüchen gingen im Berichtszeitraum mehrfach Beschwerden hinsichtlich der Löschung oder Sperrung personenbezogener Daten beim Beauftragten für den Datenschutz bei der Landeszentrale ein. In zahlreichen Fällen bemängelten Beschwerdeführer, dass sie bei Anbietern um die Löschung ihrer Daten gebeten hätten, was jedoch nicht erfolgt sei.
Dabei ist zu beachten, dass in vielen Fällen eine Löschung nicht möglich ist, solange der Löschung andere gesetzliche Vorgaben wie beispielsweise Aufbewahrungsfristen entgegenstehen. In diesen Fällen sieht § 35 Abs. 3 BDSG (alt) vor, dass an die Stelle der Löschung eine Sperrung tritt. In den aufgetretenen Fällen konnten derartige Missverständnisse bei Bürgern ausgeräumt und bei Unternehmen auf eine korrekte Umsetzung des Lösch- bzw. Sperrverlangens hingewirkt werden.

5.1.6 Datenschutzverstöße bei Werbung

5.1.6.1 Unerlaubte/unerwünschte Werbung

Auf mindestens gleichbleibend hohem Niveau war im Berichtszeitraum die Zahl der beschwerden über unerwünschte Werbung.
Das Interesse von Unternehmen, für sich oder ihre Produkte zu werben, ist anerkanntermaßen berechtigt. Dabei sind jedoch rechtlichen Vorgaben zu beachten, die sich je nach Kontaktweg unterscheiden. So ist eine werbliche Kontaktaufnahme per Post in der Regel zulässig, sofern kein Werbewiderspruch vorliegt. An Endverbraucher gerichtete Werbung per E-Mail oder Telefon dagegen bedarf regelmäßig einer Einwilligung des Betroffenen.

Aber auch postalische Werbung kann unzulässig sein, sofern der Empfänger deutlich macht, dass er keine Werbung wünsche, indem er beispielsweise einen direkten Widerspruch gegen den Erhalt von Werbesendungen ausspricht. In diesem Fall muss der Empfänger umgehend aus den entsprechenden Verteilern entfernt werden. Es kann zwar zwischen Werbewiderspruch und bereits in der Aussendung befindlichen Werbeschreiben zu zeitlichen Überschneidungen kommen. Ein Umsetzungszeitraum von einem Monat ist nach aktueller Rechtssprechung jedoch zu lang.

In einigen dem Beauftragen für den Datenschutz bei der Landeszentrale gemeldeten Fällen war nicht klar, wer eigentlich Absender eines Werbeschreibens war. Das Werbeschreiben war in diesen Fällen unadressiert an einen sogenannten Lettershop-Anbieter übermittelt worden, durch den aus eigenen Datenbanken unter Berücksichtigung von Zielgruppenvorgaben des Werbetreibenden die Schreiben adressiert und versandt wurden. Für Werbetreibende ist es in solchen Fällen ratsam, ihre Schreiben so zu gestalten, dass der eigentliche Absender und damit die für die Datenverarbeitung verantwortliche Stelle erkennbar ist.

Unabhängig von datenschutzrechtlichen Vorgaben stellt Telefonwerbung gegenüber Verbrauchern gem. § 7 Abs. 2 Nr. 2 UWG eine unzumutbare Belästigung dar, wenn keine vorherige ausdrückliche Einwilligung vorliegt, und ist damit unzulässig. Auch Werbung mittels Fax oder E-Mail ist gem. § 7 Abs. 2 Nr. 3 UWG als unzumutbare Belästigung zu werten, wenn nicht die dort in Abs. 3 aufgeführten Voraussetzungen erfüllt sind.

Ausblick:
Die Einwilligung ist gem. § 4 Abs. 1 BDSG (alt) eine mögliche Grundlage, um personenbezogene Daten rechtmäßig verarbeiten zu dürfen. Auch die DS-GVO sieht dies in Art. 6 Abs. 1 lit. a vor. Während § 4a BDSG (alt) jedoch die Schriftform vorsieht, wird diese durch die DS-GVO nicht gefordert. Es wird der verantwortlichen Stelle überlassen, wie das Zustandekommen der Einwilligung später nachgewiesen werden kann. Bei einer nicht nachweisbaren Einwilligung wird man im Zweifel zu der Annahme kommen müssen, dass in dem jeweiligen Fall die Einwilligung fehlte.
Es empfiehlt sich daher gerade künftig, das Zustandekommen von Einwilligungen entsprechend zu dokumentieren.

5.1.6.2 Bestätigungsmails mit Werbezusätzen

Die Zusendung von E-Mails mit werblichen Inhalten an Verbraucher ohne Einwilligung ist wie oben ausgeführt i.d.R. unzulässig. Dies gilt, wie durch aktuelle Rechtsprechung bestätigt, auch für werbliche Zusätze zu automatisch generierten E-Mails.
Es ist demnach unzulässig beispielsweise eine automatische Empfangsbestätigung mit einem Werbezusatz zu versehen, wenn keine Einwilligung für die Nutzung der Daten zu werblichen Zwecken vorliegt. Dies gilt auch bereits für die Bestätigungsmail, die im Rahmen eines Double-Opt-In-Verfahrens versendet wird. Nach Ansicht des BGH wird hier die elektronische Post „in zweifacher Hinsicht – nämlich für die nicht zu beanstandende Eingangsbestätigung und unzulässig für Zwecke der Werbung – genutzt. Für die Annahme, die Nutzung der elektronischen Post des Klägers sei durch die zulässige Bestätigungs-E-Mail insgesamt gerechtfertigt, bestünde indes kein Raum.“[129]
Werbetreibende Anbieter sollten künftig verstärkt darauf achten, werblichen Inhalte nicht an Verbraucher zu senden, die keine nachweisbare Einwilligung erteilt haben oder die ih-

[129] Vgl. BGH, Urteil vom 15.12.2015 - VI ZR 134/15

re Einwilligung widerrufen haben. Auch werbliche Inhalte in E-Mail-Signaturen oder an vergleichbaren Stellen sind kritisch zu hinterfragen.

5.2 Datenpannen

5.2.1 Allgemeines

Der europäische wie auch der Bundesgesetzgeber haben sich in den letzten Jahren mehrmals der Frage angenommen, wie mit Datenpannen umzugehen ist, bei denen personenbezogene Daten unrechtmäßig an Dritte übermittelt werden oder diesen unrechtmäßig zur Kenntnis gelangen. In § 42a BDSG (alt) waren für die Rechtslage im Beichtszeitraum die wesentlichen für den nicht-öffentlichen Bereich maßgeblichen Vorgaben niedergelegt.

5.2.2 Beschreibung der Vorkommnisse

Im aktuellen Berichtszeitraum ereigneten sich zwei Datenpannen i.S.d. § 42a BDSG (alt).

Im ersten Fall war es möglich, dass im Kundenbereich des Internetauftritts eines Anbieters die Daten anderer Kunden eingesehen werden konnten. Grundlage für die Fehlzuordnung waren neben bestimmten technischen Voraussetzungen auf Nutzerseite eine bestimmte Konfiguration der Sicherheitseinstellungen des Browsers. Diese Kombination führte dazu, dass die aktuell laufende Sitzung nicht mehr korrekt zugeordnet werden konnte.

Der anderere Fall betraf von einem Anbieter versandte Vertragsbestätigungsschreiben, die an falsche Adressaten verschickt worden waren. Die in den Vertragsunterlagen aufgeführten Daten waren als personenbezogen einzustufen. Zu einem geringen Anteil waren auch sensible Daten, wie z.B. Bank- und Finanzdaten betroffen.

Der Beauftragte für den Datenschutz bei der Landeszentrale war wie in vergleichbaren Fällen der Vergangenheit so auch diesen Fällen umgehend unterrichtet worden. Die weiteren gesetzlich vorgesehenen Formalien eines solchen Verfahrens waren ebenfalls eingehalten worden. Die Datenlecks konnten binnen kurzer Zeit nach ihrer Entdeckung geschlossen werden. Weitere Maßnahmen wurden im Nachgang erörtert und zeitnah ergriffen. Weiterhin war sicherzustellen, dass ausreichende technische und organisatorische Maßnahmen die erforderliche Sicherheit für die Zukunft gewährleisten.

5.3 Informationen für Anbieter

Da die die Anbieter betreffenden datenschutzrechtlichen Fragestellungen insgesamt stetig umfangreicher und gelegentlich auch brisanter werden, erscheint es sinnvoll, die Anbieter über aktuelle Entwickelungen von Zeit zu Zeit bei entsprechendem Anlass in besonderer Weise zu informieren. Die jeweilige Form wird den Anlässen angepasst und kann daher durchaus unterschiedlich ausfallen und von der individuellen Auskunft über Sammelauskünfte und Informationsschreiben bis zu Rundschreiben an alle Anbieter oder deren Datenschutzbeautragte und Informations- bzw. Schulungsveranstaltungen für diese reichen.

5.3.1 Rundschreiben an alle Anbieter zur Vorbereitung auf die Umsetzung der DS-GVO

Nach einem mehrjährigen Gesetzgebungsverfahren nahte mit dem Ablauf einer zweijährigen Übergangsphase der Zeitpunkt, ab welchem die maßgeblichen Fragen des Datenschutzrechtes nicht mehr nach deutschen Rechtsvorgaben, sondern nach den neuen für ganz Europa einheitlich geltenden Regelungen der EU-Datenschutz-Grundverordnung zu beantworten sind. Zur Vorbereitung auf diese tiefgreifenden Rechtsänderungen wurde im Herbst 2017 an alle von der Landeszentale genehmigten Anbieter ein Rundschreiben versandt, in dem die wesentlichen Grundzüge und die bedeutsamsten Neuerungen, die mit der DS-GVO einhergehen, dargestellt wurden. Damit verbunden wurden Hinweise und Handlungsempfehlungen, die den Übergangsprozess bzw. die Vorbereitung auf denselben für die Anbieter erleichtern sollten.

Nach der zum 25.05.2018 auslaufenden Übergangsphase von zwei Jahren waren die Regelungen der DS-GVO als unmittelbar geltendes Recht in allen Mitgliedstaaten der EU zu beachten.
In Bayern waren die damit erforderlich gewordenen Anpassungen landesrechtlicher Vorschriften einschließlich der Vorgaben für die dann geltenden Aufsichtsstrukturen vom Gesetzgeber bereits intensiv erwogen und erörtert worden, waren aber verbindlich erst kurz vor dem Auslaufen der Übergangsphase beschlossen worden. Insoweit konnten Hinweise nur mit der in einer solchen Situation gebotenen Zurückhaltung erfolgen.

Hinsichtlich der ab dem 25.05.2018 geltenden materiellen Rechtslage wurden folgende Themenbereiche näher beleuchtet, die bereits im Vorfeld des oben genannten Umstellungsdatums zur Vorbereitung auf die Umsetzung der DS-GVO in den Unternehmen untersucht und bei den Planungen für die Zukunft berücksichtigen werden sollten:

1. Verantwortlichkeit
Der Verantwortliche ist der zentrale Ansprechpartner nach der DS-GVO und wird als die Person oder Stelle definiert, die über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet (Art. 4 Nr. 7 DS-GVO); ihn treffen insbesondere **umfas-**

sende Rechenschaftspflichten. Er hat etwa nachzuweisen, dass die nach der DS-GVO geltenden **Grundsätze für die Verarbeitung personenbezogener Daten eingehalten** werden (Art. 5 Abs. 2 DS-GVO).

2. Technisch organisatorische Maßnahmen

Der Verantwortliche hat zudem durch geeignete **technisch-organisatorische Maßnahmen** die Einhaltung der neuen gesetzlichen Vorgaben sicherzustellen (Art. 24 Abs. 1, 25, 32 DS-GVO).

Der Verantwortliche hat unter ähnlichen Bedingungen wie bisher einen **Datenschutzbeauftragten** zu benennen, ein **Verzeichnis von Verarbeitungstätigkeiten** zu führen, in bestimmten Fällen **Datenschutz-Folgenabschätzungen** vorzunehmen und bei der Ausgestaltung der Verarbeitungsprozesse den Grundsätzen des **Privacy by Design / Privacy by Default** (Art. 25 Abs. 1 und Abs. 2 DS-GVO) zu genügen. Die Arbeitsprozesse in den Unternehmen sollten daher frühzeitig an diese Vorgaben angepasst werden.

3. Auftragsdatenverarbeitung

Die Auftragsdatenverarbeitung nach dem BDSG hat als Auftragsverarbeitung Eingang in die DS-GVO gefunden und unterliegt dort ähnlichen Regeln. Dies gilt insbesondere für die in diesem Zusammenhang abzuschließenden Vereinbarungen und den dabei zu beachtenden Mindestinhalt. Allerdings treffen den Auftragsverarbeiter künftig eine höhere Verantwortung und mehr Pflichten, z.B. zusätzliche Meldepflichten (Art. 33 Abs. 2 DS-GVO).

4. Verzeichnis von Verarbeitungstätigkeiten

Es erschien empfehlenswert, rechtzeitig ein vollständiges Verzeichnis der Verarbeitungstätigkeiten zu erstellen, denn dieses bildet letztlich die Basis, auf der der Verantwortliche seinen Verpflichtungen und insbesondere seinen Rechenschaftspflichten nach Art. 5 Abs. 2 DS-GVO nachkommen kann.

Das Verzeichnis sollte zudem auch eine Beschreibung der getroffenen technischen und organisatorischen Maßnahmen enthalten (Art. 32 Abs. 1 DS-GVO). Neu ist, dass kein öffentliches Verzeichnis mehr zu führen ist; allerdings ist das Verzeichnis der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

5. Transparenz, Informationspflichten und Rechte der Betroffenen

Der Verantwortliche hat geeignete Maßnahmen zu treffen, um den Betroffenen die geforderten Informationen (Art. 13, 14 DS-GVO) wie etwa über die Betroffenenrechte (Art. 15 bis 22 DS-GVO) und die Benachrichtigungspflicht des Verantwortlichen bei Datenschutzverletzungen (Art. 34 DS-GVO) in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Dieses Thema und die sich daraus ergebenden praktischen Folgerungen beschäftigten Unternehmen und Aufsicht jedenfalls in der Anfangszeit intensiv.

6. Sicherheit der Verarbeitung

Nach Art. 32 DS-GVO sind zur Gewährleistung eines angemessenen Schutzniveaus der Stand der Technik, Implementierungskosten, Art, Umfang, Umstände, Zweck der Verarbeitung, unterschiedliche Eintrittswahrscheinlichkeiten und Schwere des Risikos für die

Rechte und Freiheiten natürlicher Personen zu beachten. Die Kriterien dienen zur Bemessung geeigneter Maßnahmen, um ein dem Risiko der Verarbeitung angemessenes Schutzniveau zu bieten.

7. Datenschutzfolgeabschätzung (DSFA)
Eine der wichtigsten Neuerungen der DS-GVO für Deutschland ist die Datenschutz-Folgenabschätzung (DSFA). Die DSFA ist durchzuführen, wenn die Verarbeitung, insbesondere bei Verwendung neuer Technologien aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben. Dabei sind die Risiken der Verarbeitungsvorgänge abzuschätzen („Schwellwertanalyse"). Im Mittelpunkt der Risikoanalyse steht der Betroffene.
Die Aufsichtsbehörden sind gehalten, nicht abschließende Listen mit Verarbeitungstätigkeiten zu erstellen, bei denen eine DSFA durchzuführen ist.

8. Meldepflichten
Nach dem vormaligen Recht waren so genannte Datenpannen nach § 42a BDSG (alt) unverzüglich zu melden. Die Schwelle für die Meldung lag allerdings relativ hoch; bei den betroffenen Daten musste es sich um sensible personenbezogene Daten, d.h. etwa um Bank- oder Gesundheitsdaten handeln und zudem musste eine schwerwiegende Beeinträchtigung für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen.

Nach neuer Rechtslage (Art. 33, 34 DS-GVO) sind diese Hürden deutlich abgesenkt. Die Meldung hat zwar nurmehr innerhalb von 72 Stunden an die Aufsichtsbehörde (Art. 33 DS-GVO) zu erfolgen, ist aber bei jeder Verletzung des Schutzes personenbezogener Daten abzugeben. Die Pflicht entfällt nur dann, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Wann diese Voraussetzungen erfüllt sind bzw. es hieran gerade fehlt, ist seit der Einführung der DS-GVO Inhalt zahlreicher Erörterungen.

5.3.2 Informationsveranstaltung zur DS-GVO für die Anbieter

Zur weiteren Vorbereitung auf den 25.05.2018 fand im März 2018 eine Informationsveranstaltung fürleitende Personen und Datenschutzbeauftragte von Anbietern in der Landeszentrale statt.

Es zeigte sich, dass der Informationsbedarf auf Seiten der Anbieter ebenso groß war wie die Bereitsschaft, zur Umsetzung der DS-GVO entsprechende Maßnahmen zu ergreifen. Dementsprechend groß war die Resonanz dieser Veranstaltung. Zunächst wurde das neue Europäische Datenschutzrecht ausgehend von seiner Entstehungsgeschichte in seinen Grundzügen erörtert und die wesentlichen Neuerungen durch die DS-GVO vorgestellt und eingeordnet. Im einem zweiten Teil wurden im Vorfeld aus dem Kreis der Anbieter gesammelte Fragestellungen insbesondere zu den Themenbereichen der künftigen Aufsichtssituation, dem Begriff der personenbezogenen Daten bzw. der Einwilligung, zu ge-

setzlichen Erlaubnistatbeständen, zur Auftragsverarbeitung, zu Auskunfts- und Rechenschaftspflichten, Vertraulichkeitsschutz und Art. 95 DS-GVO erörtert und soweit möglich beantwortet.

5.3.3 Rundschreiben zur Anwendbarkeit des TMG nach dem 25. Mai 2018

Ein zweites Rundschreiben, das im Umfeld des 25. Mai 2018 versandt wurde, befasste sich mit der Frage, ob die vor allem im Onlinebereich besonders bedeutsamen Datenschutzregeln des TMG[130] auch nach dem Inkrafttreten der DS-GVO noch angewendet werden könnten oder durch den Anwendungsvorrang der DS-GVO überlagert würden.

Diese Frage betrifft zahlreiche Datenverarbeitungsprozesse i.V.m. der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen, also in aller Regel auch die Nutzung von Onlineverbindungen zur Rundfunkübertragung, sich daran anschließende Prozesse z.B. im Rahmen von HbbTV, die Nutzung von Webseiten aber auch Prozesse des E-Mailverkehrs. Ihre praktische Bedeutung erlangt diese Frage insbesondere durch § 15 TMG, der für Nutzungsdaten und vor allem Nutzungsprofile Erlaubnistatbestände enthält, die über diejenigen der DS-GVO in bestimmten Bereichen deutlich hinausgehen.

Wegen des prinzipiellen Anwendungsvorranges der DS-GVO als europäischem Recht gegenüber nationalem Recht der Mitgliedstaaten kann eine Fortgeltung dieser Regeln des TMG nur in Betracht kommen, wenn das Europarecht eine solche Fortgeltung anordnen würde. In Betracht kommt hierfür Art. 95 DS-GVO, der das Verhältnis der Vorgaben der DS-GVO zu Regelungszusammenhängen betrifft, die sich auf die ePrivacy-Richtlinie stützen können. Nach den ursprünglichen Planungen hätte diese Richtlinie zeitgleich mit dem Inkrafttreten der DS-GVO durch eine ePrivacy-Verordnung ersetzt werden sollen, was aber nicht geschah, weil sich der Gesetzgebungsprozess nachhaltig verzögerte.

Die Konferenz der Datenschutzbehörden des Bundes und der Länder (DSK) hat zu dieser Frage ein Positionspapier beschlossen und veröffentlicht, das den Anbietern zusammen mit dem Rundschreiben übersandt wurde.

Nach Auffassung der DSK stellen die Datenschutzregelungen des TMG vorrangig eine Umsetzung der durch die DS-GVO abgelösten EU-Datenschutzrichtlinie und daneben allenfalls eine unvollständige Umsetzung der oben angesprochenen ePrivacy-Richtlinie dar. Im Ergebnis bedeutet dies, dass die datenschutzrechtlichen Vorschriften des TMG auf automatisierte Verarbeitungen personenbezogener Daten ab dem 25. Mai 2018 keine Anwendung mehr finden können, sondern durch die DS-GVO verdrängt werden.

---

[130] Vgl. oben 2.3.2

Für diese Rechtsauffassung und seine Anwendung auf den Rundfunk spricht der Umstand, dass die Landesgesetzgeber im 21. Rundfunkänderungsstaatsvertrag die bisher vorgesehene Anwendung der Datenschutzregeln des TMG mit der Begründung aufgehoben haben, dass für das Anbieter-Nutzer-Verhältnis im Rundfunk künftig anstelle der §§ 11 ff TMG die DS-GVO unmittelbar gelte. Der Rundfunkgesetzgeber geht somit offenbar jedenfalls im Ergebnis von der Rechtsauffassung der DSK aus. Folgt man dieser Auffassung, so wird sich bis zu einem Inkrafttreten der ePrivacy-Verordnung die datenschutzrechtliche Beurteilung auch der o.g. Vorgänge an der DS-GVO ausrichten müssen. Eine rechtmäßige Verarbeitung personenbezogener Daten kann dann nur in Betracht kommen, wenn für die Verarbeitung eine gültige Einwilligung oder eine entsprechende Rechtsgrundlage der DS-GVO vorliegt.

6 Weiterbildung

Die kontinuierliche Weiterbildung im Zuständigkeitsbereich des Beauftragen für den Datenschutz bei der Landeszentrale beruhte auf dem laufenden Studium periodisch erscheinender Fachliteratur, dem Besuch von Fortbildungs- und Fachveranstaltungen zu den verschiedensten Aspekten des Datenschutzes und dem Kontakt zu anderen Datenschutzinstitutionen. Hierzu zählten im Berichtszeitraum insbesondere die Veranstaltungen der Gesellschaft für Datenschutz und Datensicherheit e.V. und darunter vor allem der Sitzungen des Erfa-Kreises Bayern. In diesen werden einerseits ausgewählte Institutionen und Firmen in Vorträgen und Erfahrungsberichten, ihre besonderen Aufgabenschwerpunkte und die dabei zu beachtenden und zu bewältigenden datenschutzrechtlichen Herausforderungen vor- und zur Diskussion gestellt. Andererseits werden in diesen Veranstaltungen allgemeine und speziellere datenschutzrechtliche Fragestellungen erörtert und fachlich bewertet, sowie von fachkundiger Seite über die aktuelle Rechtsentwicklung berichtet.

Eine besondere Bedeutung kam Veranstaltungen zu, die sich in verschiedenster Form und mit unterschiedlichen Aufgabenstellungen und Zielsetzungen mit Fragen der Rechtsfortbildung und insbesondere mit den Inhalten, Vorteilen, Schwächen und Folgewirkungen der Datenschutz-Grundverordnung befassten. Aber auch die Frage der Datensicherheit erlangt eine stetig wachsende Bedeutung und erfordert eine laufende Befassung und Fortbildung. Kontakte zu Bayerischen Sicherheitsbehörden sind hierbei sehr hilfreich wie auch deren Veranstaltungen.

Darüber hinaus wird ein laufender Erfahrungsaustausch mit dem Bayerischen Landesamt für Datenschutzaufsicht in Ansbach und werden Kontakte zum Bayerischen Landesbeauftragten für den Datenschutz wie auch zum für Datenschutzrecht zuständigen Referat des Bayerischen Staatsministerium des Innern gepflegt.

7 Schlussbemerkung

Gerade die letzten Jahre haben gezeigt, dass die vom BayMG gewählte Grundkonstruktion des Beauftragten für den Datenschutz bei der Landeszentrale nicht nur verfassungsrechtlich erforderlich ist und auch von den Anbietern angenommen wird, sondern auch zutreffende Lösungen für neu entstehende Herausforderungen fördert. Dies gilt insbesondere für die Institution des rundfunkrechtlichen Datenschutzbeauftragten, der über einen besonderen Bezug zu und spezielle Kenntnisse von der Arbeit der Anbieter und ihren Umfeldbedingungen verfügt, zudem aber auch eine intensive Erfahrung mit rundfunkrechtlichen Zusammenhängen und Fragestellungen einbringen kann. Andererseits besitzt er aber auch die verfassungsrechtlich geforderte Unabhängigkeit, die den Rundfunkbereich insgesamt auszeichnet.

Der Umstand, dass die so innerhalb des Rundfunksystems geschaffene Datenschutzkompetenz in Bayern unterdessen auch in bundesweiten Zusammenhängen genutzt wird und die zugrunde liegende gesetzliche Konstruktion zumindest im Ergebnis zwischenzeitlich auch bei anderen Landesmedienanstalten übernommen wird, ohne dass diese den der Landeszentrale eigenen Rundfunkveranstalterstatus besitzen, spricht für die Vorzüge des durch das BayMG gewählten Ansatzes, der in Bayern unterdessen im Rahmen der durch die DS-GVO notwendig gewordenen Anpassungen der Rechtslage konsequent fortentwickelt wurde.[131]

Da die Verknüpfung von Rundfunk und Telemedien fortschreitet, die Unterscheidbarkeit dieser beiden Angebotsformen zusehends schwieriger wird, und diese Fragen auch im Zuständigkeitsbereich der Landeszentrale unterdessen erheblich an Bedeutung gewonnen haben, entwickeln sich gerade in diesem Bereich der Konvergenz der Medien und Übertragungsnetze neue rundfunkrechtliche Fragen, die intensive Bezüge zum Datenschutz aufweisen. Für eine sachgemäße Lösung dieser Fragen erscheinen daher Kenntnisse und Erfahrungen sowohl im Rundfunkrecht wie auch im Datenschutzrecht ebenso sinnvoll wie wünschenswert.

Dies gilt für die Zukunftsthemen der Regulierung von (Medien-)Plattformen und ggf. künftig auch Medienintermediären ebenso wie für die Entwicklungen im Onlinebereich und unter den Stichworten Smart-TV und HbbTV, die wegen ihrer intensiven rundfunkrechtlichen Bezüge einer Lösung bedürfen, die Besonderheiten des Rundfunks aufnimmt und ihnen gerecht wird.

---

[131] Vgl. die Neufassung des Art. 20 BayMG im Rahmen des Bayerischen Datenschutzgesetzes vom 15.05.2018, GVBl 8/2018, S. 230, 254 f.