Bayerische Landeszentrale für neue Medien

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

(Berichtszeitraum: 01.01.2014 bis 31.12.2015)

I N H A L T S V E R Z E I C H N I S

1. Vorbemerkung

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

Der vorliegende Bericht ist der zwölfte Tätigkeitsbericht seit Inkrafttreten des BayMG am 01.12.1992 und bezieht sich auf die Jahre 2014 und 2015.

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 auch in den Jahren 2014/2015 aufgetretenen Datenpannen. Daneben erlangte im Berichtszeitraum das Thema HbbTV und Datenschutz eine besondere Bedeutung. Weiterhin virulent war die Frage, welche Sicherheitsanforderungen sich aus Datenschutzvorgaben ergeben, und wie hierauf im täglichen Umgang wie 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 sich auch die Rahmenbedingungen in diesem Zusammenhang deutlich verschoben haben.

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[1], dürfen nach den Vorschriften der Art. 25 und 26 EU-Datenschutzrichtlinie[2] personenbezogene Daten ins außereuropäische Ausland nur übermittelt werden, wenn beim Empfänger ein angemessenes Datenschutzniveau gewährleistet ist. Ein solches Datenschutzniveau wird auch dann angenommen, wenn ein Staat die Datenschutzkonvention des Europarats ratifiziert und Stellen eingerichtet hat, welche diese umsetzen. Für die Vereinigten Staaten galt bisher das Safe Harbour-Abkommen (Entscheidung 2000/520)[3], das nach zweieinhalbjährigen Verhandlungen zwischen der EU-Kommission und den Vereinigten Staaten im Jahr 2000 ins Leben gerufen worden war. Amerikanische Unternehmen konnten sich auf die Regelungen des Abkommens verpflichten und sich in die Safe Harbour-Liste eintragen lassen und waren somit zertifizierte Unternehmen. Das Abkommen stieß jedoch im Laufe der Jahre vermehrt auf Kritik, da die Vermutung nahe lag, dass die amerikanischen Unternehmen die Vorgaben nicht adäquat umsetzen würden. Daraufhin verlangte die deutsche Datenschutzaufsicht (vgl. Beschluss des Düsseldorfer Kreises vom 11./12.09.2012[4]), dass deutsche Unternehmen eine Prüfung amerikanischer Handelspartner in zwei Stufen vornehmen, um eine sichere Übermittlung in Drittstaaten zu gewährleisten, solange eine flächendeckende Kontrolle der Selbstzertifizierung US-amerikanischer Unternehmen durch die Kontrollbehörden in Europa und den USA nicht gewährleistet sei. Inzwischen stellte der EuGH jedoch mit Urteil vom 06.10.2015 fest, dass das Safe Harbour-Abkommen zwischen den USA und der EU ungültig ist[5].

Der Entscheidung des EuGH lag ein Rechtsstreit des Österreichers Max Schrems mit der irischen Datenschutzbehörde zugrunde, die wegen des Sitzes 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[6]. 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

---

[1] 11. Tätigkeitsbericht des Beauftragten für den Datenschutz bei der Bayerischen Landeszentrale für neue Medien S. 6
[2] Richtlinie 95/46/EG, Amtsblatt Nr. L 281 vom 23.11.1995 S. 0031-0050
[3] Entscheidung der Kommission vom 26. Juli 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
[4] http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/12092013DatenuebermittlungInDrittstaaten, vgl.11. Tätigkeitsbericht S. 6,7
[5] EuGH Urt. v. 06.10.2015, C-362/14 (Schrems) in BayVBl. 2016, 193 ff.
[6] EuGH a.a.O. Rn. 28

der Kommission[7] die Möglichkeit haben müssen, die Rechtmäßigeit der Datenübermittlung in die USA zu überprüfen[8]. Zudem stellte der EuGH fest, dass die Safe Harbour-Entscheidung der Kommission inhaltlich unzutreffend und daher ungültig sei[9].

Denn für den EuGH stand eindeutig fest, dass, wenn aufgrund des US-amerikanischen Rechts US-Unternehmen eine den Grundsätzen des sicheren Hafens entgegenstehende Verpflichtung auferlegt wird, die US-Unternehmen diese Gesetze einhalten müssen und zwar ungeachtet dessen, ob sie auf die Grundsätze des sicheren Hafens verpflichtet sind oder nicht[10]. Aufgrund dieses Vorrangs der amerikanischen Gesetzte sind US-Organisationen, die aus der Union personenbezogene Daten erhalten, ohne jede Einschränkung verpflichtet, die Grundsätze des "sicheren Hafens" unangewandt zu lassen, wenn sie in Widerstreit zu den Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen stehen[11]. Im Ergebnis laufe die Safe Harbour-Regelung daher ins Leere[12].

Hinzu kam, dass es für die betroffenen Unionsbürger in der USA keine Regeln gebe, etwaige Eingriffe zu begrenzen, und es gebe auch keinen wirksamen gerichtlichen Rechtsschutz gegen derartige Eingriffe[13]. Im Ergebnis sah der EuGH daher durch die so geschaffenen Verhältnisse den Wesensgehalt der europäischen Grundrechte auf Achtung des Privatlebens und des wirksamen gerichtlichen Rechtsschutzes als verletzt an.

Am 15.10.2015 hat die Artikel-29-Datenschutzgruppe ein Statement[14] und am 21.10.2015 die Konferenz der unabhängigen Datenschutzbehörden (DSK) ein Positionspapier[15] herausgegeben, die folgende Eckpunkte enthalten:

Datenübermittlungen aufgrund der Safe Harbour-Entscheidung sind unzulässig. Sofern eine Datenschutzaufsichtsbehörde Kenntnis eines solchen Datentransfers in die USA erhält, wird sie diese untersagen.

Die Mitgliedstaaten und die europäischen Datenschutzinstitutionen sind aufgefordert mit den US-amerikanischen Behörden Gespräche zu führen,

---

[7] 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)
[8] EuGH a.a.O. Rn. 38-78
[9] EuGH a.a.O. Rn. 79-106
[10] EuGH a.a.O. Rn. 85
[11] EuGH a.a.O. Rn. 86
[12] EuGH a.a.O. Rn. 88
[13] EuGH a.a.O. Rn. 89
[14] https://datenschutz-berlin.de/attachments/1154/statement_Art_29.pdf?1448010649
[15] http://www.lfd.niedersachsen.de/download/101387/Positionspapier_der_Datenschutzbeauftragten_vom_26.10.2015_zum_Safe-Harbor-Urteil_des_EuGH.pdf.

um politische, rechtliche und technische Lösungen zu finden, damit die Grundrechte bei Datenübermittlungen in das Hoheitsgebiet der USA gewahrt werden.

Die nationalen Datenschutzbehörden werden derzeit keine neuen Genehmigungen für Datenübermittlungen in die USA aufgrund von Standardvertragsklauseln oder Binding Corporate Rules erteilen.

2.1.2 Datentransfers in die USA nach der Safe Harbour-Entscheidung des EuGH[16]

Mit dem Urteil des EuGH vom 06.10.2015 zum Safe Harbour-Abkommen stand eigentlich fest, dass auf der Grundlage geltenden europäischen Rechts ein zulässiger Transfer von personenbezogenen Daten, für welche ein gewisses Maß an Schutzwürdigkeit der Betroffenen besteht, nur noch schwer vorstellbar war. Auch eine Übermittlung auf der Grundlage von Standardvertragsklauseln oder Binding Corporate Rules, die formal von der o.g. EuGH-Entscheidung nicht betroffen waren, konnte auf der Grundlage der Feststellungen des EuGH nur noch schwerlich als materiell rechtmäßig angesehen werden.

2.1.2.1 EU-US Privacy Shield

Um die wohl weiterhin laufend stattfindenden Datentransfers in die USA wieder auf eine tragfähige rechtliche Basis zu stellen, hat die EU-Kommission unmittelbar nach der Safe Harbour-Entscheidung des EuGH Verhandlungen mit der US-Regierung aufgenommen, die letztlich, wenn auch erst im Jahr 2016, ein sogenanntes EU-US Privacy Shield hervorbrachten. In der Sache handelt es sich wohl um ein informelles Übereinkommen, in dessen Rahmen die vormalige US-Regierung zusagte, dass nunmehr EU-Bürgern eine Klagemöglichkeit in den USA eröffnet werde, wenn diese eine Verletzung des Datenschutzes geltend machen wollten.

Dabei 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. EU-Bürger könnten sich an einen Ombudsmann beim amerikanischen Außenministerium wenden, um Verstößen nachzugehen und prüfen zu lassen, ob ein

[16] Vgl. oben 2.1.1 EuGH Urt. v. 06.10.2015, C-362/14 (Schrems); BayVBl. 2016, 193 ff.

Unternehmen rechtswidrig gehandelt habe.

Gleichwohl steht zu befürchten, dass weiterhin eine flächendeckende und anlasslose Überwachung von EU-Bürgern stattfindet[17] und die mögliche Beschwerde bei dem o.g. Ombudsmann, einem Beamten des amerikanischen Außenministeriums, letztlich doch keine für die Wahrung europäischer Grundrechte hinreichende Rechtsschutzmöglichkeiten darstellt.

2.1.2.2 Transatlantische Handels- und Investitionspartnerschaft (TTIP)

Die EU und die USA verhandeln seit 2011 über ein Freihandelsabkommen, das unter dem Kürzel TTIP[18] 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.

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 geben bisher die EU-

[17] Vgl. die Stellungnahme des Art. 29 Datenschutzgruppe vom 13.04.2016
[18] http://www.bmwi.de/DE/Themen/Aussenwirtschaft/Ttip/faqs.html

Datenschutzrichtlinie[19] sowie die E-Privacy-Richtlinie (RL 2002/58/EG)[20] den zu beachtenden Rechtsrahmen vor, die die Harmonisierung der sich aus dem Datenschutz ergebenden Anforderungen im Hinblick auf einen einheitlichen Wirtschaftsrahmen als Ziel verfolgen.

Unterdessen ist eine EU-Datenschutz-Grundverordnung (DS-GVo) zwischen den maßgeblichen EU-Organen Kommission, Parlament und Rat abgestimmt und beschlossen worden, und wird im Mai 2018 in allen EU-Mitgliedstaaten einheitlich verbindlich inkrafttreten. Diese DS-GVo wird danach die meisten datenschutzrechtlichen Fragestellungen für das gesamte Gebiet der EU, alle seine Bürger und Unternehmen und zum Teil auch für die staatlichen Institutionen neu und weitgehend abschließend regeln[21].

2.2.1 Der 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[22] 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**[23] 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 Mitgliedsstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Unionsrecht fallen. Die inzwischen verabschiedete Datenschutz-Grundverordnung[24] ist eine Umsetzung dieser Vorgaben.

- Die wohl wichtigste Änderung bestand jedoch in der Bezugnahme auf die Charta der Grundrechte. In **Art. 8 der Grundrechtecharta**[25] ist

[19] RL 95/46/EG, ABl. EG v. 23.11.1995, Nr. L 281/31
[20] Im Telekommunikationsbereich wird die Datenschutzrichtlinie durch die im Jahr 2002 erlassene RL 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) ergänzt.
[21] Vgl. unten 2.2.2
[22] 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).
[23] Vertrag über die Arbeitsweise der Europäischen Union
[24] Vgl. unten 2.2.2.
[25] Art. 8 Schutz personenbezogener Daten
(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

zum ersten Mal auf europäischer Ebene rechtsverbindlich ein **Grundrecht auf Datenschutz** normiert. Was dies für die Geltung deutscher Grundrechte bedeutet, insbesondere ob die europäischen Grundrechte ein vergleichbares Schutzniveau gewährleisten[26], ist ebenso umstritten wie die zu erwartenden Folgen einer diese ausgestaltenden Datenschutz-Grundverordnung.

Der für Datenschutzfragen bisher zuständige Bundesverfassungsrichter Prof. Masing[27] 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.

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 war, kann wohl nur entstehen, wenn die neu geschaffenen europäischen Rechte, die gleichen Rechtsgüter schützen oder zumindest eine sehr ähnliche Zielrichtung verfolgen.

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.

2.2.2 EU-Datenschutz-Grundverordnung

2.2.2.1 Allgemeines

Nachdem bereits am 06.12.2011 ein erster inoffizieller Entwurf im Internet veröffentlicht worden war[28], hat die Europäische

---

(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.

[26] Vgl. *Ronellenfitsch*, Der Vorrang des Grundrechts auf informationelle Selbstbestimmung vor dem AEUV, DuD, 2009, S. 451 ff.

[27] Johannes Masing, "Ein Abschied von den Grundrechten", SZ 29.01.2012

[28] http://www.statewatch.org/news//2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf

Kommission am 25.01.2012 den Entwurf einer europäischen Datenschutz-Grundverordnung[29] offiziell vorgelegt, der seither im Europäischen Parlament und im Rat unter den Mitgliedstaaten intensiv erörtert und teilweise auch sehr kontrovers diskutiert wurde.

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 Übergangsphase, in der die nationalen Gesetzgeber Zeit haben, ihre nationalen Regeln dem neuen Rechtszustand anzupassen, ab dem 25.05.2018 einheitlich in allen Mitgliedstaaten gelten werden. Die Datenschutz-Grundverordnung wird die bisherige EU-Datenschutzrichtlinie 95/46/EC ersetzten und den Datenschutz im gesamten nicht-öffentlichen und auch öffentlichen Bereich weitgehend bestimmen. Dem zentralen Anliegen, einen einheitlichen europäischen Datenschutzstandard zu schaffen, folgend sind von diesen Regeln sowohl die Landeszentrale selbst wie auch die bei ihr genehmigten Anbieter unmittelbar betroffen. Das neue europäische Recht gilt unmittelbar für beide, enthält aber für den öffentlichen Bereich etwas mehr Spielräume, die die nationalen Gesetzgeber für ihren Bereich individuell ausformen können.

Eine solche Öffnungsklausel ergibt sich insbesondere 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 Mitgliedsstaaten für diese Zwecke das Recht einräumt, Abweichungen und Ausnahmen von den Regeln der DS-GVo vorzusehen.

Die bisher geltenden Datenschutzregeln des Bundes und der Länder werden aktuell einer grundlegenden Überarbeitung unterzogen, die nahezu alle Bereiche erfasst und vom BDSG über das BayDSG bis hin zum BayMG reicht. Bis zum 25.05.2018 werden die bisher geltenden Vorgaben grundlegend überarbei-

[29] 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) – v. 25.01.2012, KOM (2012)/11 endgültig.

tet und zahlreichen Veränderungen unterzogen werden.

2.2.2.2 Inhalte der Verordnung

Inhaltlich sieht die Datenschutz-Grundverordnung einen vergleichsweise robusten Individualdatenschutz vor, der das **Prinzip der Einwilligung** des Betroffenen ins Zentrum des neuen Rechtes stellt. Dies ist einerseits sicherlich zu begrüßen, bildete andererseits aber auch einen Kernpunkt der Kritik, die dies für eine unausgewogene Überbetonung des Individualdaten- und des Persönlichkeitsrechtschutzes hält.

Die Datenschutz-Grundverordnung räumt Betroffenen aber 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 bereits unter Geltung des derzeitigen Rechts grundgelegt. Der Verbraucher soll ggf. seine Einwilligung auch wieder zurückziehen können und damit das Recht haben, dass auf seinen Wunsch hin ihn betreffende persönliche Daten wieder gelöscht werden. Für die Praxis geht man wohl weitgehend davon aus, dass dies nur schwer umsetzbar sein und daher letztlich doch nur einen qualifizierten Löschungsanspruch darstellen wird.

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 Strafen von bis zu vier Prozent des Jahresumsatzes. Ob diese Strafandrohung in der Praxis tatsächlich die erwartete Bedeutung gewinnen wird, wird sich erst noch zeigen müssen.

Eine der zentrale Neuerungen ergibt sich aus dem europaweiten Ansatz der Datenschutz-Grundverordnung, denn mit ihrer Einführung sollten die rechtlichen Rahmenbedingungen für Fragen des Datenschutzes in ganz Europa einheitliche werden. 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 die Möglichkeit einer in allen Datenschutzfragen für dieses Unternehmen zuständigen 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

Diese unterschiedlichen Ansichten wie auch die Interessen der Internetwirtschaft einerseits und die bisher in Deutschland vorherrschende Vorstellung von einem vor allem individuellen Grundrechtsschutz auf informationelle Selbstbestimmung andererseits in der Zukunft zu einem Ausgleich zu bringen, wird eine der wesentlichen Aufgaben der künftigen Rechtsanwendung sein.

Ob dies gelingen kann, ist derzeit nur schwer zu prognostizieren. Zu groß sind die bisher geweckten Erwartungen und zu wenig konkret die gesetzlichen Vorgaben, als dass zum gegenwärtigen Zeitpunkt verlässliche Voraussagen hierzu möglich wären. Andererseits enthält die Datenschutz-Grundverordnung auch sehr viele Ansätze, um viele der in Aussicht genommenen Zielsetzungen jedenfalls hinreichend zu verwirklichen. Gegenwärtig unternehmen die deutschen Gesetzgeber große und vor allem auch sehr intensive Anstrengungen, die deutsche Rechtslage bis zum endgültigen Wirksamwerden der Datenschutz-Grundverordnung im Mai 2018 auf die dann geltende europaweite Rechtslage abzustimmen und auch organisatorisch alle notwendigen Vorarbeiten zu erledigen. Dass ihnen Großes gelingen möge, ist ihnen und den Bürgern zu wünschen.

2.2.3 Zulässigkeit der Vorratsdatenspeicherung

Mit der Richtlinie 2006/24/EG[30] des Europäischen Parlaments und des Rates vom 15.03.2006 wurden die EU-Mitgliedsstaaten verpflichtet, dafür Sorge zu tragen, dass von Anbietern von Telekommunikationsdiensten Verbindungsdaten verschiedenster Kategorien mindestens sechs Monate auf Vorrat gespeichert werden[31]. Erste Klagen gegen diese Richtlinie hatte der EuGH noch zurückgewiesen[32], dabei aber Aussagen zu einer möglichen Verletzung von Grundrechten bewusst vermieden.[33]

In Deutschland wurde die o.g. Richtlinie per Gesetz in 2007 umgesetzt [34]; dieses wurde durch das Bundesverfassungsgericht mit Urteil vom 02.03.2010[35] als mit dem Grundgesetz unvereinbar verworfen.[36] Eine Neuregelung scheiterte zunächst an Meinungsverschiedenheiten innerhalb der damaligen Bundesregierung[37]. Im Koalitionsvertrag vom Dezember 2013 vereinbarten CDU, CSU und SPD sodann, die Richtlinie zur Vermeidung von Zwangsgeldern doch umzusetzten.[38]

Im April 2014 entschied der EuGH, dass die o.g. Richtlinie gegen die EU-Grundrechtecharta verstoße[39]. Es war der Ansicht, dass ein unzulässiger Eingriff insbesondere in die Grundrechte des Telekommunikationsgeheimnis, auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten vorliege.

Im Mai 2015 wurde dennoch der Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherpflicht für Verkehrsdaten vorgelegt[40], der zwar von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder kritisiert wurde[41]; dennoch hat der Bundestag das Gesetz in der vom Rechtsausschuss geänderten Fassung[42] beschlossen,

---

[30] ABl. EG v. 15.03.2006, Nr. L 105/54
[31] Vgl. Art. 3 i.V.m Art. 6 der RL 2006/24/EG
[32] EuGH Urt. v. 10.02.2009, Az: C-301/06
[33] 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.
[34] Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer versteckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, BGBl. 2007 I Nr. 70 S. 3198 ff.
[35] BVerfG Urt. v. 02.03.2010, BVerfGE 125, 260 ff.
[36] 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.
[37] Vgl. Möstl, Zeitschrift für Rechtspolitik 2011, S. 226
[38] 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."
[39] Vgl. EuGH Urt. v. 08.04.2014, C-293/12 und C-594/12; K&R 2014, 405 ff.
[40] BR-Drs. 249/15
[41] Umlaufentschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09.06.2015
[42] BT-Drs. 186391

das somit am 18.12.2015 in Kraft trat[43].

Mit Urteil vom 21.12.2016[44] hat der EuGH sich nochmals mit nationalen Regeln zur Vorratsdatenspeicherung befasst und diesmal schwedische und britische Vorschriften zur Vorratsdatenspeicherung für ungültig erklärt, die allerdings eine allgemeine und unterschiedslose Speicherung von Daten vorsahen. Dabei hat er aber auch 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[45].

2.2.4 Richtlinie 2009/136/EG[46]

Am 25.11.2009 haben das Europäische Parlament und der Rat der Europäischen Union mit der Richtlinie 2009/136/EG u.a. Vorgaben der sogenannten E-Privacy-Richtlinie[47] verschärft und Informationspflichten für den Fall einer Verletzung des Schutzes personenbezogener Daten geschaffen[48]. Diese Informationspflichten sind weitergehender als die bisher[49] vorgesehenen. Die Diensteanbieter werden zudem verpflichtet, ein Verzeichnis der Verletzungen des Schutzes personenbezogener Daten zu führen. Die Umsetzung[50] der Richtlinie erfolgte in der Novelle zum TKG vom 09.05.2012[51].

Zudem enthält diese RL 2009/136/EG aber auch die Vorgabe[52], eine Speicherung von Informationen oder den Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, im Wesentlichen nur zu gestatten, wenn der betreffende Teilnehmer oder

---

[43] BGBl. 2015 I Nr. 51 S. 1324 ff.; vgl. unten 2.3.5
[44] EuGH Urt. v. 21.12.2016, C-203/15 und C-698/15.
[45] 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 konkrete 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.
[46] RL2009/136/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
[47] Datenschutzrichtlinie für elektronische Kommunikation, RL 2002/58/EG
[48] Z.B. hat der Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste nach dem neuen Art. 4 Abs. 3 der E-Privacy-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.
[49] Z.B. in § 42a BDSG, § 15a TMG und § 93 Abs. 3 TKG
[50] Die eigentliche Frist zur Umsetzung in nationales Recht lief bis zum 25.05.2011
[51] BGBl. 2012 I Nr. 19 S. 958 ff.
[52] Über eine Änderung von Art. 5 Abs. 3 der RL 2002/58/EG, der sog. E-Privacy-Richtlinie

Nutzer auf der Grundlage von klaren und umfassenden Informationen u.a. über die Zwecke der Verarbeitung seine Einwilligung gegeben hat.

Diese Vorgaben hat Deutschland bis heute nicht umgesetzt, weshalb diese Richtlinie in Deutschland unmittelbar anwendbar sein könnte. Bedeutung erlangt diese Frage, weil diese Richtlinie nicht von der DS-GVo verdrängt wird[53].

2.2.5 Urteil des EuGH vom 13.05.2014: Google Spain

Mit diesem Urteil[54] hat der EuGH Google verpflichtet, Links auf von Dritten veröffentlichte Informationen in den Ergebnislisten ihrer Suchmaschine unter bestimmten Voraussetzungen zu entfernen. 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 unter einer veränderten Rechtslage gültig sein dürften.

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.

Der EuGH stufte einerseits das Betreiben einer Suchmaschine, die automatisch im Internet veröffentlichte Informationen aufspürt, als eigene Erhebung von Daten ein, 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 Europa befindlichen Niederlassung erfolgt, wenn diese Niederlassung die Aufgabe der Vermarktung der Werbeflächen der Suchmaschine wahrnimmt.

Schließlich wurde eine Verpflichtung dieser Suchmaschinenbetreiber 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

[53] Vgl. Art. 95 DS-GVo mit Erwägungsgrund 173
[54] EuGH Urt. v. 13.05.2014, C-131/12

als solche rechtmäßig ist[55], weil die Rolle des Internets und der Suchmaschinen in einer modernen Gesellschaft eine besondere ist und den in den Ergebnislisten enthaltenen Informationen Ubiquität verleiht.

2.3 Bundesrecht

2.3.1. Bundesdatenschutzgesetz (BDSG) - Beschäftigtendatenschutz

Der Arbeitnehmerdatenschutz ist seit langem ein Thema, wenn auch der letzte deutsche Gesetzesentwurf[56] vom August 2010 stammt. Das Gesetz wurde jedoch bis zum Ende der damaligen Legislaturperiode nicht verabschiedet.

Im aktuellen Koalitionsvertrag einigten sich CDU, CSU und SPD darauf, 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.[57]

Die Regelungen der DS-GVo haben den Beschäftigtendatenschutz letztlich weitgehend ausgespart und überlassen ihn abgesehen von sehr allgemein gehaltenen Vorgaben der Regelung durch die Mitgliedstaaten[58].

2.3.2 Telekommunikationsgesetz (TKG)

Im Jahr 2012 waren die EU-Richtlinien 2009/140/EG[59] und 2009/136/EG[60] umzusetzen. Dies erfolgte mit Gesetz vom 03.05.2012[61]. Danach erfolgten Änderungen im TKG vor allem durch das IT-Sicherheitsgesetz[62] und das Gesetz zur Einführung einer Speicherfrist und einer Höchstspeicherdauer für Verkehrsdaten[63], die unter 2.3.4 und 2.3.5 dargestellt werden.

2.3.3 Telemediengesetz (TMG)

Im Berichtszeitraum wurden Veränderungen im TMG vor allem durch das IT-Sicherheitsgesetz[64] vorgenommen, das unter 2.3.4 dargestellt wird.

[55] EuGH Urt. v. 13.05.2014 C-131/12 Rdnr. 62
[56] Gesetzesentwurf Bundesregierung; BR-Drs. 535/10
[57] Koalitionsvertrag v. 16.12.2013 S. 50
[58] Vgl. Art. 88 DS-GVo und Erwägungsgrund Erwägungsgrund 155
[59] RL 2009/140/EG, ABl. L 337 v. 18.12.2009, 37
[60] RL 2009/136/EG, ABl. L 337 v. 18.12.2009, 11
[61] BGBl. 2012 I Nr. 19, S. 958 ff.
[62] BGBl. 2015 I Nr. 31, S. 1324 ff.
[63] BGBl. 2015 Nr. 51 S. 2218 ff.
[64] BGBl. 2015 I Nr. 31 S. 1324 ff.

Daneben hätte eigentlich die Richtlinie 2009/136/EG [65] und die darin enthaltene Änderung des Art. 5 Abs. 3 der E-Privacy-Richtlinie (2002/58/EG), die den Einsatz von Cookies beschränkt und ihren Gebrauch von der vorherigen Einwilligung des Nutzers abhängig macht, bis zum Mai 2011 umgesetzt werden müssen.[66] Hierzu hatte der Bundesrat am 17.06.2011 einen Gesetzesentwurf beschlossen[67], der umfangreiche Änderungen im TMG vorsah[68]. Die Bundesregierung sah in dem Gesetzesentwurf zwar wichtige Themen angesprochen, hielt aber einige hiervon für zunächst klärungsbedürftig wohl auch im Hinblick auf die künftige DS-GVo[69], so dass es zu keiner Umsetzung kam.

Die mittlerweile beschlossene DS-GVo wird das TMG in maßgeblichen den Datenschutz betreffenden Teilen überlagern, jedoch nicht soweit das TMG die E-Privacy-Richtlinie (2002/58/EG) umsetzt[70].

2.3.4 IT-Sicherheitsgesetz

Das Bundesministerium des Inneren veröffentlichte am 05.03.2013 den Entwurf des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), das Änderungen an zahlreichen Gesetzten, insbesondere am BSI-Gesetz[71] vorsieht. Das Gesetz wurde am 12.06.2015 vom Bundestag beschlossen und ist nach Zustimmung des Bundesrats am 25.07.2015 in Kraft getreten[72].

Das Gesetz verpflichtet Betreiber kritischer Infrastrukturen[73], 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). Welche Unternehmen letztlich wirklich verpflichtet sein werden, wird eine Verordnung des Bundesinnenministeriums regeln. Möglicherweise werden

---

[65] S.o. Fn. 49
[66] S.o. 2.2.4
[67] BR Drs. 156/11
[68] So sollen z.B. die Informationspflichten der Diensteanbieter gegenüber den Nutzern verstärkt werden, Datenschutzhinweise sollen in allgemeinverständlicher Form, leicht erkennbar und unmittelbar erreichbar sein. Es soll für Nutzer jederzeit und ohne technisches Hintergrundwissen die Möglichkeit bestehen, datenschutzrechtliche Informationen zu erhalten. Standardmäßig sollen bei Neuanmeldungen zunächst die höchsten Sicherheitsstufen voreingestellt sein, die nur vom Nutzer gelockert werden können, und es soll eine wichtige Voreinstellung geben, die die Auffindbarkeit und Auslesbarkeit mittels externer Suchmaschinen verhindert. Zudem sollen die Nutzer durch Aufklärung hinsichtlich der Risiken der Veröffentlichung persönlicher Daten sensibilisiert werden. Letztlich soll der Nutzer immer die Gelegenheit haben, seine in dem Telemediendienst veröffentlichten Daten wieder zu löschen oder zumindest zu sperren oder zu anonymisieren.
[69] vgl. Art. 95 DS-GVo mit Erwägungsgrund 173, der das künftige Zusammenspiel mit der E-Privacy-Richtlinie (2002/58/EG) regelt.

[70] Die Richtlinie (2002/58/EG) gilt wegen Art. 95 DS-GVo auch künftig, vgl. oben 2.2.4
[71] BSI-Gesetz v. 14.08.2009 (BGBl 2009 I Nr. 54, S. 2821 ff.)
[72] BGBl. 2015 I Nr. 31 S. 1324 ff.
[73] 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.

Rundfunkverteilnetze unter diese Regelungen fallen; ob Rundfunkanbieter hierzu auch zählen können, bleibt abzuwarten. Landesmedienanstalten dürften aber unmittelbar von diesen Vorgaben nicht betroffen sein.

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 wird 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[74]. 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[75].

2.3.5 Gesetz zur Einführung einer Speicherfrist und einer Höchstspeicherdauer für Verkehrsdaten vom 17.12.2015[76]

Nach der langen Vorgeschichte der Vorratsdatenspeicherung[77] und eingehenden Diskussionen auf allen Ebenen trat am 18.12.2015 das Gesetz zur Einführung eine Speicherfrist und einer Höchstspeicherdauer für Verkehrsdaten in Kraft.

Inhaltlich verpflichtet das Gesetz Telekommunikationsunternehmen, Internet-Provider und andere Zugangsanbieter u.a. dazu, so genannte Verkehrsdaten zehn Wochen lang zu speichern. Die Standortdaten, welche im Rahmen der Nutzung von Mobil-Diensten anfallen, sollen vier Wochen gespeichert werden. Von den Regelungen sind ausgenommen Berufsgeheimnisträger wie Rechtsanwälte, Ärzte und Journalisten, deren Daten zwar mitgespeichert werden, jedoch nicht verwertet werden dürfen. Im Rahmen des Gesetzes ist auch der Straftatbestand der "Datenhehlerei[78]" eingeführt worden.

Ziel sei, die Aufklärung schwerer Straftaten und die Gefahrenabwehr zu erleichtern, wofür Verkehrsdaten ein wichtiges Hilfsmittel für die staatlichen Behörden seien.[79] Es gehe zum Beispiel um die Rufnummern beteiligter Anschlüsse sowie Zeit und Ort eines Gesprächs. Es gehe nicht um

[74] Vgl. § 100 Abs.1 TKG
[75] 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
[76] BGBl. 2015 I Nr. 51 S. 2218 ff.
[77] S.o. 2.2.3
[78] S.u. 2.3.6
[79] http://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/Einfuehrung_Speicherfrist_Hoechstspeicherfrist_Verkehrsdaten.html

die Inhalte der Telekommunikation.

Die Zulässigkeit einer solchen Regelung wird mit Verweis auf zahlreiche entgegenstehende Grundrechte bestritten, was zu einer Reihe von Verfassungsbeschwerden geführt hat. Als Begründung wird häufig angeführt, dass die Speicherung v.a. der Standortdaten in Verbindung mit der Protokollierung der IP-Adressen den Bürger transparent mache; man könne so letztlich den ganzen Tagesablauf der Mehrheit der Bürger nachvollziehen. Zudem würden auch Berufsgeheimnisträger und deren Daten erfasst, die aber auf eine vertrauliche Kommunikation angewiesen seien.[80] Ein anderer Begründungsstrang stützt sich auf die Rechtsprechung des EuGH[81], die die anlasslose und flächendeckende Speicherung von Daten in der Regel als unverhältnismäßig ansieht.[82]

2.3.6 Datenhehlerei (§ 202d StBG)

Zusammen mit dem o.g. Gesetz zur Einführung einer Speicherfrist und einer Höchstspeicherdauer für Verkehrsdaten vom 17.12.2015[83] wurde mit dem neuen § 202d StGB der Straftatbestand der Datenhehlerei geschaffen.

Begründet wurde dies damit, dass mit der sich rasant entwickelnden Informationstechnologie der Handel mit rechtswidrig erlangten digitalen Daten wie z.B. Kreditkartendaten oder Zugangsdaten zum Onlinebanking, E-Mail-Diensten oder sozialen Netzwerken immer 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[84] den neuen Tatbestand erfordere. Zur wirksamen Bekämpfung der Cyberkriminalität sieht der Gesetzentwurf konsequenterweise auch eine Erhöhung der Strafrahmen für das Ausspähen und Abfangen von Daten (§§ 202a, 202b StGB) vor.

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.

---

[80] https://netzpolitik.org/2016/verfassungsbeschwerde-gegen-die-vorratsdatenspeicherung-mit-ueber-32-000-unterzeichnern/
[81] Vgl. oben 2.2.3
[82] https://netzpolitik.org/2016/weitere-verfassungsbeschwerde-gegen-vorratsdatenspeicherung-eingereicht/
[83] Vgl. oben 2.3.5
[84] BVerfGE 120, 274 ff.

2.3.7 Bundesmeldegesetz

Um erstmals bundesweit einheitliche und unmittelbar geltende melderechtliche Vorschriften für alle Bürger und Bürgerinnen zu schaffen, wurde ein Entwurf für ein Bundesmeldegesetz auf den Weg gebracht. Nach einer 1. Lesung am 26.04.2012 wurde der Gesetzesentwurf am 28.06.2012 in zweiter und dritter Lesung – wohl vor leeren Parlamentssitzen während eines EM-Fußball-Halbfinalspieles[85] – beraten und beschlossen. In dieser Fassung war es den Meldebehörden erlaubt, persönliche Daten von Bürgern an Firmen zu verkaufen, sofern nicht ausdrücklich ein Widerspruch der Betroffenen vorlag. Daran entzündete sich eine öffentliche Diskussion über die Weitergabe von Meldedaten an Dritte.

Der Bundesrat rief am 21.09.2012 den Vermittlungsausschuss an, in dem sich Bund und Länder einigten, die Notwendigkeit der Einwilligung wieder einzuführen. Das Bundesmeldegesetz wurde am 28.02. bzw. 01.03.2013 beschlossen, am 08.05.2013[86] verkündet und ist am 01.05.2015 in Kraft getreten.

Unterdessen ist das Bayerische Gesetz zur Ausführung des Bundesmeldegesetzes (BayAGBMG) vom 23.06.2015 am 01.11.2015 in Kraft getreten. Hierzu wurde die Meldedatenverordnung vom 15.09.2015, die ebenfalls zum 01.11.2015 in Kraft getreten[87] ist, erlassen.

2.4 Bayerisches Landesrecht

2.4.1 Änderung des Bayerischen Datenschutzgesetzes (BayDSG)

Das bayerische Datenschutzgesetz wurde aufgrund des Bayerischen E-Gouvernement-Gesetzes vom 22.12.2015[88] in mehreren Punkten[89] verändert. Die wesentlichste Veränderung bildete aber die Einführung des Art. 36 BayDSG, mit dem ein allgemeines Recht der Bürger auf Informationszugang gegenüber öffentlichen Stellen in Bayern eingeführt wurde. Art. 36 wurde in den neu gebildeten siebten Abschnitt des BayDSG aufgenommen, was das Ziel des Gesetzgebers unterstrich, mit einer allgemeinen Informationszugangsregelung im BayDSG die bisherigen Anforderungen zum Schutz personenbezogener Daten nicht zu verschlechtern.[90]

[85] Vgl. Abel, Das neue Melderecht, RDV 2013, S. 179
[86] BGBl. 2013 I Nr. 22, S. 1084 ff.
[87] BayGVbl. Nr. 11/2015 S. 357-370
[88] BayGVbl. Nr. 17/2015
[89] Betroffen waren die Art. 4, 15, 26, 27a und 28
[90] Vgl. Komm. zum BayDSG Wilde Ehmann Niese Knoblauch Stand 26. EL Oktober 2016 Art. 36 Rdnr. 3

Erlaubt wird die Auskunft über personenbezogene Daten somit erst dann, u.a. wenn keine schutzwürdigen Interessen durch den Betroffenen entgegenstehen. Auch wenn bisher die Auswirkungen der Neuregelung auf die behördliche Praxis eher gering sind[91], hat der Landesgesetzgeber doch ein klares Signal zugunsten von Transparenz und Partizipation gesetzt.

2.4.2 Rundfunkstaatsvertrag

Die im Berichtzeitraum erfolgten Änderungen des Rundfunkstaatsvertrages entfalteten keine datenschutzrechtlichen Wirkungen.

2.4.3 Rundfunkgebührenstaatsvertrag – Popularklageverfahren vor dem Bayerischen Verfassungsgerichtshof

Der 15. Rundfunkänderungsstaatsvertrag wurde von den Regierungschefs im Dezember 2010 unterzeichnet und fristgemäß zum 31.12.2011 von den Länderparlamenten ratifiziert. Er trat am 01.01.2013 in Kraft[92]. Der Rundfunkbeitragsstaatsvertrag (RBStV) sieht seither vor, dass pro Haushalt bzw. Betriebsstätte ein Beitrag entrichtet wird, mit dem alle Nutzungsmöglichkeiten abgegolten sind. Hinsichtlich der Frage, ob bei diesem neuen Ansatz auch 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, da Nachforschungen beim Betroffenen minimiert würden und sich der Einsatz von Rundfunkgebührenbeauftragten deutlich reduzieren lasse. 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. Insgesamt würden langfristig nur die Daten Zahlungspflichtiger gespeichert[93]. Die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder angemahnte Nachbesserung der Staatsvertragsregeln zur Beachtung der Erforderlichkeit, Verhältnismäßigkeit, Normklarheit und Datensparsamkeit ist vom Gesetzgeber bisher nicht für erforderlich gehalten worden.

---

[91] Vgl. Will in BayVbl. 2016, 620

[92] Einige Übergangsvorschriften in § 14 Abs. 1, 2 und 6 des Rundfunkbeitragsstaatsvertrag (RBeitrStV) galten sogar bereits seit dem 01.01.2012.

[93] Vgl. auch die Eckpunkte von ARD, ZDF und Deutschlandradio für eine Konkretisierung der datenschutzrechtlichen Regelungen im Vollzug des 15. RÄndStV vom November 2011.

Seit 2012 waren gegen verschiedene Bestimmungen des RBStV Popularklagen anhängig. Der Bayerische Rundfunk, die Bayerische Landeszentrale für neue Medien, das Zweite Deutsche Fernsehen und das Deutschlandradio hielten diese für unbegründet. Der bayerische Verfassungsgerichtshof hat die Klagen mit Urteil vom 15.05.2014[94] abgewiesen.

Aus datenschutzrechtlicher Sicht ging es vor allem um die Vorschrift zum einmaligen Datenabgleich gem. § 14 Abs. 9 RBStV, die der Verfassungsgerichtshof für verfassungsgemäß hielt. Die Vorschrift ermögliche es, die bereits für den früheren Rundfunkgebühreneinzug gespeicherten Daten einmalig zum Inkrafttreten des neuen Rundfunkbeitragsmodells mit dem Melderegister abzugleichen und zu vervollständigen, um eine möglichst lückenlose Bestands- und Ersterfassung im privaten Bereich zu erreichen.[95] Der Eingriff in das Recht der informationellen Selbstbestimmung sei gerechtfertigt, um ein Vollzugsdefizit und die Herstellung größerer Beitragsgerechtigkeit für legitime Zwecke herzustellen.

2.4.4 Bayerisches Mediengesetz

Die im Berichtzeitraum erfolgten Änderungen im Bayerischen Mediengesetz entfalteten keine datenschutzrechtlichen Wirkungen.

3. Funktion des Beauftragten für den Datenschutz

Mit Art. 20 BayMG als bereichspezifischer Datenschutznorm hat 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 trägt und andererseits ausdrücklich das Medienprivileg aufnimmt, hat sich nachhaltig bewährt.

Durch den Beauftragten für den Datenschutz bei der Landeszentrale können die spezifischen Anforderungen im Bereich des in öffentlich-rechtlicher Trägerschaft betriebenen Rundfunks gewährleistet werden, da einerseits ein hohes Maß an Sachkenntnissen bezüglich der rechtlichen, wirtschaftlichen und programmlichen Verhältnisse besteht. Andererseits stellt die gewählte Gestaltung aber auch sicher, dass bei der Rechtsanwendung die spezifischen Bedingungen des Rundfunks wie auch die bestehenden verfassungsrechtlichen Besonderheiten Berücksichtigung finden.

Zudem entfällt so die ansonsten erforderliche, im Einzelfall aber immer schwierige und

[94] BayVGH Urt. v. 15.05.2014, Az. Vf. 8-VII-12 und Vf. 24-VII-12
[95] BayVGH a.a.O.

auch problematische Abgrenzung zwischen Erhebung, Verarbeitung und Nutzung personenbezogener 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 überwacht gem. Art. 20 Abs. 3 Satz 2 BayMG die Einhaltung der Vorschriften des BayMG sowie anderer Vorschriften über den Datenschutz bei der Landeszentrale und bei den Anbietern umfassend[96], und zwar auch, soweit es sich um Verwaltungsangelegenheiten handelt.[97] Mit dieser umfassenden Zuständigkeit für alle Aufgaben bei der Landeszentrale und den Anbietern trägt das BayMG den verfassungsrechtlichen Anforderungen an einen rundfunkrechtlichen Datenschutz Rechnung.[98]

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

Der Beauftragte hat bei der Durchführung seiner Aufgaben Auskunfts-, Kontroll-, Zugriffs-, Einsichts- und Beanstandungsrechte.[99] Der Beauftragte für den Datenschutz bei der Landeszentrale ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Ein solcher unabhängiger Datenschutzbeauftragter ist vor allem im Hinblick auf die Überwachung der Datenschutzregelung nach Art. 20 Abs. 2 BayMG für den journalistisch-redaktionellen Bereich notwendig, aber auch zweckmäßig. Da der Beauftragte für den Datenschutz unabhängig und nur dem Gesetz unterworfen ist, können keine Weisungen, insbesondere auch nicht vom Präsidenten oder dem Verwaltungsrat erteilt werden, die sich auf seine inhaltliche Aufgabenerfüllung beziehen. Die Stellung des Beauftragten entspricht damit der des Bayerischen Landesbeauftragten für Datenschutz bzw. des Präsidenten des Landesamtes für Datenschutzaufsicht.

Die Ausgestaltung der Datenschutzaufsicht nach dem BayMG entspricht somit auch zweifelsfrei den Anforderungen des Europarechtes[100] einschließlich der EU-Datenschutzrichtlinie[101], die in Art. 28 Abs. 1 den Mitgliedsstaaten auferlegt, datenschutzrechtliche Kontrollstellen zu schaffen, die die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahrnehmen. Dies gilt prinzipiell auch für die Anforderungen, die sich ab dem Mai 2018 aus der dann zu beachtenden EU-DS-GVo ergeben werden, die auch die Rechtsstellung der Datenschutzaufsichtsinstitutionen neu regelt, zumal

---

[96] 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.

[97] Vgl. Art. 20 Abs. 3 Satz 3 BayMG.

[98] 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."

[99] Vgl. insbes. Art. 20 Abs. 4 BayMG.

[100] Art. 8 Abs. 3 EU-Grundrechtecharta wie auch Art. 16 Abs. 2 AEUV sehen eine Beaufsichtigung durch unabhängige Stellen zwingend vor.

[101] RL 95/46/EG, ABl. EG v.23.11.1995, Nr. L 281/31.

sich zahlreiche diesbezügliche Anforderungen bereits aus der EU-Grundrechtecharta[102] ergeben, und daher selbstverständlich weiterhin zu beachten sind.[103]

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

Insbesondere besteht keine Einordnung des Beauftragten für den Datenschutz bei der Landeszentrale in den durch den Präsidenten der Landeszentrale geleiteten Verwaltungsaufbau. Der Präsident beruft zwar den Beauftragten für den Datenschutz bei der Landeszentrale, bedarf hierfür aber der Zustimmung des Verwaltungsrates.[104]

Im Übrigen bestehen 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 ist dennoch Teil der Landeszentrale und Ausdruck ihrer staatsfernen Selbstverwaltung, was die interne Dienstaufsicht durch den Verwaltungsrat unterstreicht.

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.

Der Digitalausschuss wurde zur "Datenschutz-Problematik bei HbbTV und Smart-TVs" in einer seiner Sitzung eingehend unterrichtet.

---

[102] Vgl. insbesondere Artikel 8 GrR-Ch zum Schutz personenbezogener Daten und zur Unabhängigkeit der diesbezüglichen Aufsicht.

[103] So z.B. die Feststelllungen des EuGH im Urt. v. 09.03.2010, C- 518/07 zu der Frage, was Unabhängigkeit in diesem Zusammenhang bedeutet.

[104] Vgl. Art. 20 Abs. 3 Satz 1 BayMG.

Im Rahmen des Rechtssymposiums der Landeszentrale referierte der Beauftragte vor einem vorwiegend juristischen Fachpublikum zum Thema "Datenschutzprobleme bei der Individualisierung von Medieninhalten".

Der Fachausschuss I der ZAK wurde in Berlin mit einem Vortrag zu dem Thema "Datenschutzaufsicht in Deutschland und insbesondere im Rundfunk" über die Struktur der Deutschen Datenschutzaufsicht und die Besonderheiten der in Zuständigkeitsfragen zu beachtenden gesetzlichen und verfassungsrechtlichen Vorgaben unterrichtet.

"Die neue Technik und der Datenschutz" war der Titel eines Vortrages im Rahmen einer Tagung der AG Katholischer Frauen Bayerns, die in Kooperation mit dem Bildungswerk des Bayerischen Landesverbandes des KDFB e.V. zu dem Thema "Big Data – Wen hole ich mir denn da ins Wohnzimmer?" in der Landeszentrale stattfand.

Schließlich wurde ein weiterer Vortrag mit dem Titel "Alte Inhalte – Neue Sehgewohnheiten: Wie wird das Fernsehen der Zukunft aussehen. Was bedeutet das für den Datenschutz" im Rahmen einer Veranstaltung der Evangelischen Frauen in Bayern in der Landeszentrale gehalten.

4.1.1 Datenschutzrechtliche Freigabe automatisierter Verfahren nach Art. 26 BayDSG

Die Landeszentrale ist gem. Art. 26 Abs. 1 BayDSG 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 ist kein Verfahren vorgelegt worden. Der Beauftragte bemüht sich derzeit um eine Bestandserhebung aller auch der nicht freigabepflichtigen automatisierten Verfahren, in deren Zuge personenbezogene Daten verarbeitet werden.

4.1.2 Verfahrensverzeichnis nach Art. 27 BayDSG

Die Landeszentrale führt gem. Art. 27 BayDSG ein Verzeichnis der bei ihr eingesetzten und datenschutzrechtlich freigegebenen automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden. Dieses Verfahrensverzeichnis wird jährlich fortgeschrieben. In diesem Ver-

zeichnis sind für jedes automatisierte Verfahren die in Art. 26 Abs. 2 BayDSG 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. Rügefristen 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 weitgehend sensibilisiert sind. Bei Zweifelsfragen wenden sie sich in der Regel selbständig 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 im Einzelfall 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; überwiegend stammten die Anfragen jedoch diesmal aus dem Rechtsbereich. Insgesamt war festzustellen, dass sich in den aufgetretenen Fragestellungen die mit der fortschreitender 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 speichern, zu verändern oder zu nutzen, die zur Erfüllung der in die Zuständigkeit der entsprechenden Stelle fallenden Aufgaben erforderlich sind.[105]

Daraus ergibt sich immer wieder und in unterschiedlichen Gestaltungen die Frage, in welchen Zusammenhängen bei der Landeszentrale vorhandene bzw. für bestimmte Zielsetzungen erhobenen 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.

[105] Vgl. z.B. Art. 16 Abs. 1 und Art. 17 Abs. 1 Nr. 1 BayDSG.

4.3.2 Zulässige Zweckänderung

Im Zusammenhang damit ergibt sich häufig die weitere Frage, ob und wenn ja zu welchen 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 grundlegenden Erkenntnissen deutschen Datenschutzrechtes.[106]

Aus diesem Grunde ist die Ermittlung des ursprünglichen Nutzungszweckes von besonderer Bedeutung, so dass derartige Nachfragen stets eine hohe Berechtigung besitzen. Andererseits erlaubt das für die Landeszentrale maßgebliche BayDSG zahlreiche Nutzungsänderungen[107], deren Tatbestandsvoraussetzungen im Einzelfall zu prüfen sind.

Hierbei ist jedoch auch zu berücksichtigen, dass von der Zulässigkeit einer auch veränderten Nutzung in den meisten Fällen auszugehen ist, insbesondere wenn die fraglichen Daten für Aufsichts- und Kontrollbefugnisse der Landeszentrale erforderlich sind und genutzt werden sollen.[108]

Im Berichtszeitraum waren derartige Fragen häufiger aufgetreten, wobei insbesondere die Fragen, welche Bedeutung bestehende Auskunfts – und Meldepflichten bzw. der Umstand haben, dass seinerzeit bestimmte Angaben freiwillig gemacht wurden, wie die Zulassungstätigkeit der Landeszentrale in diesem Zusammenhang einzuordnen ist, welche Folgen die oben genannten Überlegungen für Ermessensentscheidungen in unterschiedlichen Bereichen haben, und welche Bedeutung sie bei Förderentscheidungen entwickeln können, zu beantworten waren.

Insgesamt ist festzuhalten, dass Zweckänderungen durchaus häufig möglich sind; gleichwohl muss hierfür eine Einwilligung, das offensichtliche Interesse des Betroffenen oder eine gesetzliche Ermächtigungsnorm vorliegen, deren Voraussetzungen im konkreten Einzelfall jeweils überprüft werden müssen.

---

[106] Vgl. bereits das sog. Volkszählungsurteil des BVerfG vom 15.12.1983 (BVerfGE 65, 1ff.).
[107] Vgl. insbesondere Art. 17 Abs. 2 BayDSG.
[108] Vgl. Art. 17 Abs. 3 Satz 1 BayDSG.

4.3.3 Übermittlung von personenbezogenen Daten an Dritte

Immer wieder wird die Frage gestellt, welche Daten z.B. von Anbietern an Dritte übermittelt werden dürfen; häufig haben diese angefragt bzw. darum geben, bestimmte Daten übermittelt zu bekommen.

Der Standpunkt des Gesetzes wie auch der Landeszentrale hierzu ist sehr klar. Personenbezogenen Daten sind zu schützen; um solche[109] handelt es sich nur bei Daten, die sich auf natürliche Personen beziehen, nicht hingegen bei Daten einer juristischen Person. Sofern es jedoch um Daten geht, die sich zwar vordergründig auf eine juristische Person beziehen, darüber hinaus aber durchaus auch Aussagen über die "dahinterstehenden" natürlichen Personen enthalten, kann ein Personenbezug vorliegen, der den Schutzbereich des Datenschutzes eröffnet[110]. Häufig liegen solche Gestaltungen bei OHGs, KGs, nicht-rechtsfähigen Vereinen oder "Einmann-GmbHs" vor, so dass Aussagen über die dortigen z.B. finanziellen Verhältnisse auch einen Rückschluss auf die Kreditwürdigkeit des Geschäftsführers oder anderer natürlicher Person ermöglichen können.

Auch ohne namentliche Nennung bestimmter Personen ist häufig die dahinter stehende natürliche Person erkennbar. Werden zudem noch weitere Details genannt, ist in aller Regel der Rückschluss auf konkrete natürliche Personen noch einfacher möglich. Aus diesem Grund liegen bei solchen Fallgestaltungen in der Regel auch personenbezogene Daten im Sinne des Art. 4 BayDSG vor; die Vorgaben des Datenschutzes sind dann zu berücksichtigen.

Grundsätzlich ist daher mit Anfragen nach Adressen und Strukturen von Anbietern sehr vorsichtig umzugehen, die Zulässigkeit der Übermittlung im Einzelnen zu überprüfen und in der Praxis häufig zu verneinen.
Geht die Anfrage über die bloße Datenübertragung hinaus und erstreckt sich zudem auf Texte und Bilder, die weitergegeben werden sollen, ist zusätzlich auf mögliche urheberrechtliche Fragen hinzuweisen, die ebenfalls vor einer Übermittlung zu prüfen und zu klären sind.

4.3.4 IP-Adressen als personenbezogene Daten

Die Frage, ob IP-Adressen personenbezogene Daten darstellen oder nicht, war weiterhin bedeutsam und wurde intensiv diskutiert, weil einerseits IP-Adressen häufig anfallen und reichhaltige Aufschlüsse über das Nutzungsverhalten im Internet ermöglichen. Andererseits steht dahinter die Grundsatzfrage, welche Daten, die zunächst für sich betrachtet noch keinen

[109] Im Falle der Verarbeitung in der Landeszentrale im Sinne des Art. 4 BayDSG.
[110] Vgl. Komm. z. BayDSG, Wilde, Ehmann, Niese, Knoblauch, 26. EL, Stand Oktober 2016, Art. 4 Rdnr: 11.

Personenbezug aufweisen, die man aber mit unterschiedlich hohem Aufwand Personen zuordnen kann, als personenbezogen einzuordnen sind. Dies Frage ist deshalb so bedeutend, weil der Personenbezug gewissermaßen die Eintrittskarte in den Bereich des Datenschutzes darstellt, und daher die Einordnung als personenbezoges Datum darüber entscheidet, ob für diese Daten Datenschutzregeln gelten oder nicht.

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener) [111]. Die EU-Datenschutzrichtlinie 95/46/EG ergänzt, dass als bestimmbar eine Person angesehen wird, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, psychologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind[112].

In Erwägungsgrund Nr. 26 dieser Richtlinie wird zudem vorgesehen, dass alle Mittel zu berücksichtigen sind, die von dem für die Verarbeitung Verantwortlichen oder von jeder anderen Person nach vernünftiger Einschätzung zur Identifizierung der betreffenden Person genutzt werden können, um festzustellen, ob eine Person bestimmbar ist[113].

Eine IP-Adresse ist eine Ziffernfolge, die bei einer Internetnutzung entsteht. Diese gibt Auskunft, von welchem Internetanschluss in einem bestimmten Zeitraum das Internet genutzt wurde.[114] Es gibt statische IP-Adressen, hier ist der Anschluss fest zugeordnet, und dynamische IP-Adressen, die vom Accessprovider bei jeder Einwahl neu vergeben werden. Bei dynamischen IP-Adressen ist der Personenbezug streitig.[115]

Bestimmbar sind die hinter den IP-Adressen stehenden Personen zweifellos, denn die Access-Provider speichern, wem sie wann welche dynamischen IP-Adressen zuweisen. Streitig ist, ob der Schutz der Daten nur für diejenigen Personen gilt und nur diese zu einem entsprechenden Verhalten verpflichtet, die den konkreten Personenbezug kennen bzw. selbst herstellen können, oder es genügt, dass der Bezug ggf. auch nur von Dritten hergestellt werden kann.

Nach hiesiger Ansicht genügt, wie es auch das Gesetz ausdrückt, dass die betroffene Person bestimmbar ist. Dass dies für die konkret handelnde Person zum aktuellen Zeitpunkt zutreffen muss, um von einer bestimm-

[111] Diese Definition findet sich in zahlreichen deutschen Datenschutzgesetzen wie z.B. in Art. 4 Abs. 1 BayDSG oder § 3 Abs. 1 BDSG.
[112] Art. 2 Buchst. a der EU-Datenschutzrichtlinie 95/46/EG
[113] Dies hat die europäische Artikel 29-Datenschutzgruppe in ihrem Arbeitspapier Nr.159 besonders hervorgehoben.
[114] Vgl. Härting, Internetrecht, S. 22 Rdnr. 89.
[115] Vgl. Härting, CR 2008, S. 743, 745 f.

baren Person auszugehen, ist dem Gesetz nicht zu entnehmen. Zudem hätte eine solche Forderung auch weitreichende negative Folgen.

Die gegenteilige Meinung, die hierfür auf den konkreten Wissensstand der handelnden Person abstellen möchte, führt dazu, dass die betreffenden Daten solange als nicht personenbezogen und damit völlig schutzlos und somit schrankenlos handelbar wären, bis sie endlich bei einer Person anlanden, der die Zuordnung konkret möglich ist. Dies würde zu einer erheblichen Gefährdung des Datenschutzes und des dahinterstehenden Grundrechtsschutzes führen, die vom Gesetz nicht gewollt ist und sich durch eine Pseudonymisierung der erfassten Daten vermeiden lässt. Wer sich für die Person, die hinter z.B. einer dynamischen IP-Adresse steckt, nicht interessiert, kann an Stelle der IP-Adresse in der Regel ein beliebiges Pseudonym auswählen und speichern, das den ganzen Vorgang datenschutzrechtlich unproblematisch macht, gleichwohl aber den gleichen Zweck erfüllt, wenn auch später ein Personenbezug nicht hergestellt werden soll. Auf diese Sichtweise hatten sich auch die Landesdatenschutzbeauftragten jedenfalls im Ergebnis geeinigt.

Mit Beschluss vom 28.10.2014 hat der BGH[116] die Frage, ob dynamische IP-Adressen personenbezogene Daten sind, dem EuGH zur Klärung vorgelegt. Der EuGH hat mit Urteil vom 19.10.2016[117] über diese Frage entschieden. Er hält danach dynamische IP-Adressen nur dann für personenbezogen, wenn der sie speichernde Website-Betreiber "über rechtliche Mittel verfügt, die es ihm erlauben, den betreffenden Nutzer anhand der Zusatzinformationen, über die dessen Internetzugangsanbieter verfügt, bestimmen zu lassen". In der Praxis bedeutet dies, dass von personenbezogenen Daten auszugehen ist, wenn vom vergebenden Zugangsprovider Name und Anschrift des Adressinhabers zu erhalten ist. Hierzu hat der EuGH festgestellt, dass in Deutschland dafür offenbar ausreichende rechtliche Möglichkeiten in der Regel bestehen.

Damit dürfte die Frage für die deutsche Praxis zunächst dahingehend entschieden sein, dass bei IP-Adressen von personenbeziehbaren Daten auszugehen ist. Des weiteren ist dem EuGH zuzugestehen, dass die europarechtlichen Grundlagen jedenfalls bei wörtlicher Betrachtung eine solche Entscheidung nahegelegt haben. Gleichwohl bleibt die Frage offen, ob eine Beschränkung auf die in Europa bestehenden legalen Erkenntnisquellen eine abschließende zutreffende Lösung hervorbringt, denn es sind ohne weiteres Fallgestaltungen denkbar, in denen der Personenbezug für

[116] BGH Beschl. v. 28.10.2014 VI ZR 135/13, NJW 2015, 368. Der BGH wollte wissen, ob es sich bei dynamischen IP-Adressen um personenbezogene Daten im Sinne des Art. 2 lit. a RL 95/46/EG handelt, wenn nicht der Diensteanbieter selbst, sondern ein Dritter über das Wissen zur Identifizierung des Betroffenen verfügt, und ob § 15 Abs. 1 TMG weiterhin gültig sei, wonach die sogenannten Nutzungsdaten erhoben und verwendet werden dürfen, um die Inanspruchnahme von Telemedien zur ermöglichen und abzurechnen.

[117] EuGH Urt. v. 19.10.2016 C-582/14, abgedruckt in MMR 2016, 842 ff.

ganze Datenbestände aus zahlreichen Nutzungszusammenhängen von Erkenntnisquellen abhängen kann, die in Europa legal nicht zur Verfügung stehen, international aber ohne weiteres verfügbar sind.

Für solche Fälle würde die stringente Anwendung der oben genannten EuGH Entscheidung dazu führen, dass für diese Datenbestände keinerlei Datenschutzregeln zu beachten wären, die Daten daher problemlos rechtmäßig verkauft und gehandelt werden könnten, da es in der konkreten Situation ja an einem Personenbezug fehlen würde. Dies würde es ermöglichen, diese nur scheinbar unproblematischen Datenbestände ins außereuropäische Ausland zu übertragen, wo mit den dort zur Verfügung stehenden erweiterten "Erkenntnisquellen" der bisher fehlende Personenbezug hergestellt werden könnte. Dass derartige Möglichkeiten auch von der EU Grundrechte-Charta nicht gewollt sein können, sollte eigentlich auf der Hand liegen.

4.3.5 Datenschutz bei Kabelanlagenbetreibern

Zu überprüfen war weiterhin, welche datenschutzrechtlichen Gesichtspunkte Kabelanlagenbetreiber bei Angaben zu ihrer Kabelanlage und den daran angeschlossenen Wohneinheiten zu beachten haben und welche Grenzen für diesbezügliche Auskunftsverpflichtungen sich aus Datenschutzregeln ergeben.

Grundsätzlich haben Betreiber einer Kabelanlage gemäß Art. 33 BayMG diese anzuzeigen und Detailangaben zu dieser zu machen, wie z.B. den Standort der Kabelanlage, das Versorgungsgebiet, die Zahl der anschließbaren und angeschlossenen Wohneinheiten u.a.[118] Im Rahmen dieser Verpflichtung werden von der Landeszentrale weitere Angaben angefordert.

Datenschutzrechtliche Fragestellungen können sich hieraus ergeben, wenn aus diesen Angaben Rückschlüsse auf konkrete Personen möglich werden. Normalerweise scheidet dies aus, da Auskunftsverpflichtungen erst bei Kabelanlage, die der Versorgung von 10 oder mehr Wohneinheiten dienen, bestehen, so dass aus diesen Angaben i.d.R. auf keine persönlichen oder sachlichen Verhältnisse zu konkreten Personen geschlossen werden kann.

Liegen die Verhältnisse im Einzelfall anders, bedarf es entweder der Einwilligung des Betroffenen oder einer gesetzlichen Erlaubnis. Diese ist abgesehen von Ausnahmefällen dann gegeben, wenn die Kenntnis der er-

[118] vgl. Kommentar zum Bayerischen Mediengesetzt Bornemann/von Coelln/Heppach/Himmelsbach/Lörz 40. EL, Art. 33 Rdnr. 10

fragten Daten zur Erfüllung der Aufgaben der Landeszentrale erforderlich ist.[119] Ob dies tatsächlich der Fall ist, ist im Einzelfall zu ermitteln. Da Daten im Regelfall beim Betroffenen zu erheben sind und weitere Detailfragen zu beachten wären, reduzieren sich unter Beachtung dieser Vorgaben die Anwendungsfälle stark.

Datenschutzrechtliche Bedenken von Kabelanlagenbetreibern bestätigen sich umgekehrt aber jedenfalls dann nicht, wenn lediglich zusammengefasste Daten abgefragt und erhoben werden, aus denen keine Rückschlüsse auf einzelne Personen gezogen werden können.

5. Datenschutz bei den Anbietern und Tochtergesellschaften der Landeszentrale

5.1 Allgemeines

Einen maßgeblichen Teil der Tätigkeit des Beauftragten für den Datenschutz bei der Landeszentrale bildete, wie auch in den Vorjahren, die Beratung der Anbieter in Fragen des Datenschutzes und insbesondere hinsichtlich der sich aus den gesetzlichen Vorgaben ergebenden Anforderungen für die Gestaltung des betrieblichen Ablaufs. Dabei erforderte das Thema Bewältigung von Datenlecks sowie Beratungen zum Thema Smart-TV im Berichtszeitraum besonderer Aufmerksamkeit.

Inzwischen gehört die Bewältigung einer großen Anzahl von Anfragen und Beschwerden insbesondere wegen unerwünschter oder jedenfalls nicht erbetener Werbung per Post, E-Mail oder Telefon inhaltlich zu den Routineaufgaben, die aber durch die im Jahr 2014/2015 nochmals angestiegene Anzahl dennoch eine erhebliche Herausforderung darstellten. 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 der Daten 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 ausgesprochen bzw. die Löschung aller gespeicherten Daten beantragt. Auffällig war, dass Anfragen wegen Auskunftserteilung in den letzten zwei Jahren häufiger und vor allem konkreter wurden, so dass hier von den Anbietern eine detaillierte Auskunft abzugeben war.

Auch das Thema Werbung mit Teiladressierung, d.h. Werbung an die Haushalte einer bestimmten Hausnummer, war wieder verstärkt Gegenstand von Beschwerden. Aus datenschutzrechtlicher Sicht handelt es sich dabei um Postwurfsendungen und um keine persönlich adressierten Werbesendungen, d.h. es fehlt i.d.R. das Merkmal "personenbezogen" im Sinne des Bundesdatenschutzgesetzes. In

[119] Vgl. Art. 16 Abs. 1 BayDSG.

diesen Fällen ist ein Vorgehen gegen derartige Werbebotschaften im Rahmen des Bundesdatenschutzgesetzes zumeist nicht möglich. Eine Hilfestellung bietet hier lediglich der Eintrag eines Werbewiderspruchs und die Aufnahme in die interne Werbesperrliste. Eine weitere Verfolgung der Angelegenheit unter verbraucherschutzrechtlichen Gesichtspunkten bleibt jedoch selbstverständlich unbenommen.

Zumeist waren die Beschwerdeführer zunächst in unmittelbaren Kontakt mit den betroffenen Anbietern getreten. Häufig konnten die Beschwerdeführer ihre in der Regel 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, so dass sie sich zur Einschaltung des Beauftragten veranlasst sahen.

Neben den geschilderten Fällen unzulässiger Datennutzungen für Werbezwecke erstreckten sich die Beschwerden auf zahlreiche andere Fragestellungen, wie beispielsweise die Zulässigkeit von Bonitätsprüfungen oder die Rechtmäßigkeit der Weitergabe von Daten an Dritte, bis hin zu Fragen unzulässigen Datenhandels sowie die Verknüpfung mit weiteren Rechtsgeschäften, wie z.B. Abonnements.

Weiterhin waren Fragen zur Zulässigkeit der Koppelung von Vertragsschlüssen an die Einwilligung zur Werbung durch Anbieter zu klären. In bestimmten Fallgestaltungen ergab sich eine solche Kopplung bzw. der Eindruck einer solchen, der aber fast ebenso wirksam auf die Freiwilligkeit der anzugebenden Einwilligung einwirkt, aus der Gestaltung der technischen Abläufe bzw. den hierzu gegebenen Informationen. In bestimmten Fällen lag dem auch lediglich ein technisches Problem zugrunde, das sich nur bei bestimmten Endgeräten manifestierte.

Ein weiteres Thema war die Zulässigkeit von Telefonmitschnitten, die dafür erforderlichen Voraussetzungen und ihre technische Umsetzung, sowie der spätere Umgang mit diesen Mitschnitten bis hin zur Löschung derselben.

In der Regel konnte dem Beschwerdevorbringen in einem überschaubaren Zeitraum abgeholfen und die begehrte Löschung bzw. Sperrung von Daten bewirkt oder die gewünschte Auskunft bzw. Bestätigung des Bestehens oder Nichtbestehens eines Rechtsverhältnisses herbeigeführt werden. Darüber hinaus sind aber Bürgeranfragen und Beschwerden auch im Hinblick auf die Erfüllung der Aufgabe, für die tatsächliche Einhaltung der gesetzlichen Rahmenbedingungen zu sorgen, häufig sehr wertvoll.

5.2. Verletzung eines Persönlichkeitsrechts durch Filmaufnahmen

Beschwerdegegenstand war im Berichtszeitraum auch die Frage, ob bei der Herstellung ausgestrahlter Fernsehsendungen privater Anbieter Persönlichkeitsrechte von abgebildeten Personen in der besonderen Spielart von individuellen Datenschutzrechten verletzt worden waren.

Diese Frage spielt immer wieder dann eine Rolle, wenn Beiträge für Sendungen erstellt werden, die Lebenssituationen mit einer besonderen Dringlichkeit oder Brisanz für die unmittelbar Betroffenen oder Dritter zum Gegenstand haben. Die dabei gewünschte Darstellungsform steht dann nicht selten in einem nicht unerheblichen Spannungsverhältnis zu bestimmten Fragen des Persönlichkeitsrechtes der abgebildeten oder anderweitig erkennbaren und damit betroffenen Personen.

Zu prüfen waren in der Vergangeheit Fälle von Wohnungsöffnungen, Durchsuchungsmaßnahmen oder Unfallsituationen, die entweder intensive Berührungspunkte zu Persönlichkeitsrechten aufwiesen oder aber aufgrund mangelnder Verpixelung oder anderweitiger Unkenntlichmachung der gezeigten Personen bzw. ihrer individuellen Lebensumstände zu klärende Rechtsfragen mit sich brachten.

Die Fälle sind zumeist ebenso programminhaltlich wie auch datenschutzrechtlich zu bewerten, wobei trotz des ähnlichen Grundansatzes doch auch die Unterschiedlichkeiten der Rechtsmaterien zu berücksichtigen sind. In der Regel stehen jedoch die programminhaltlichen Bewertungsmaßstäbe im Vordergrund, so dass die davon unabhängige datenschutzrechtliche Bewertung in diese Prüfung eigenständig eingehen kann, dennoch aber nach außen eine einheitliche Reaktion der Landeszentrale möglich bleibt.

In diesen Fällen zeigt sich der besondere Vorzug der unabhängigen rundfunkrechtlichen Datenschutzbeauftragten.

5.3 Smart-TV und HbbTV

Die Themen Smart-TV und HbbTV beschreiben technische Neuerungen, die dem Fernsehzuschauer zusätzliche Nutzungsmöglichkeiten bieten, aber auch neue datenschutzrechtliche Fragestellungen mit sich bringen. Mit der Anschaffung und Aktivierung eines Smart-TV erhält der Zuschauer nun auch über das TV-Gerät den Zugang zum Internet, damit aber auch die mit diesem Medium üblicherweise verbundenen Fragestellungen. Ist die Verbindung zum Internet auf einem solchen Gerät aktiviert, erhält der Fernsehnutzer über HbbTV Signalisierungen zudem weitere abrufbare Inhaltsangebote über den Anbieter des jeweiligen Fernsehprogramms.

Dieses Angebot wird technisch in aller Regel bisher dadurch verwirklicht, dass das

Fernsehgeräte angeregt durch die HbbTV-Signalisierungen eine Internetverbindung zu einem Server des jeweiligen Fernsehanbieters aufbaut, dabei aber auch entsprechende Daten auf diesem Server hinterlässt. Was das insgesamt bedeuten kann bzw. welche möglichen Gefährdungen damit einhergehen können, war Gegenstand zahlreicher Publikationen, und dies wiederum Anstoß für eine intensive öffentliche Diskussion zu diesem Thema.

Im Zuge dessen haben die Landesdatenschutzbeauftragten aber auch die Landeszentrale durch den Fachbereich Technik eine Untersuchung durchgeführt, welche Datenverbindungen üblicherweise von Smart-TV-Geräten bzw. HbbTV-Signalisierungen aufgebaut und betrieben werden.

Für die datenschutzrechtliche Bewertung ist es wichtig darauf hinzuweisen, dass die mit dem Stichwort "Smart-TV" verbundenen Datentransfers entweder durch das Fernsehgeräte selbst angestoßen werden bzw. durch entsprechende Internetnutzungen ausgelöst werden. Im Gegensatz dazu handelt es sich bei den durch HbbTV-Anwendungen ausgelösten Datenübertragungen um solche, die zu einem erheblichen Teil dem Bereich des Rundfunks zuzurechnen sind, oder zumindest ursprünglich aus diesem Bereich initiiert wurden. Daraus ergeben sich zahlreiche Folgerungen für die jeweils verantwortliche Stelle und die für sie zuständige Aufsicht.

Datenschutzrechtlich erscheint es wichtig, auf Folgendes hinzuweisen:

Der Datenaustausch beginnt sogleich mit dem Einschalten des Fernsehgeräts. Diese Austauschprozesse haben in aller Regel nichts mit Fernsehprogrammen und ihren Anbietern zu tun. TV-Programme mit HbbTV-Signalisierung initiieren mit dem Aufruf des Programms auf für solche Nutzungen vorgesehenen Fernsehgeräten selbstständig weitere Datentransfers. Vom Nutzer wird in aller Regel bewusst lediglich ein linearer Dienst genutzt; in der Regel hat der Nutzer keine Kenntnis von den ausgelösten Datenübermittlungen. Alle in diesem Stadium anfallenden Daten beziehen sich auf seinen Rundfunkkonsum und nicht auf einen von ihm bewusst ausgelösten Abrufprozess.

Ein Abruf von Inhalten durch den Nutzer findet erst mit dem Drücken des Red Button statt, so dass das Drücken auf den Red Button datenschutzrechtlich eine maßgebliche Zäsur bildet; vor diesem geht es in der Regel nur um Rundfunknutzungen, so dass in aller Regel die verantwortliche Stelle der jeweiligen Fernsehanbieter ist. Danach mag sich dies ändern, da dann ein Abrufdienst genutzt wird.

Besondere Bedeutung erlangt diese Erkenntnis im Hinblick auf die durch den Einsatz dieser Technik möglich werdenden Datentransfers, die in den eingesetzten Fernsehgeräten angeregt werden können, ohne dass der jeweilige Nutzer diese bewusst angestoßen hätte oder auch nur Kenntnis von ihnen erlangt. Zudem lassen sich aus diesen Daten Nutzungsprofile zu den einzelnen Fernsehgeräten und

in Kombination mit anderen Informationen gegebenenfalls auch zu einzelnen Nutzern anlegen.

Wegen der grundsätzlichen Bedeutung dieser Thematik für die künftige Rundfunkentwicklung, aber auch für die dabei zu berücksichtigenden Grundrechtspositionen der Fernsehnutzer fand ein reger Austausch zu diesen Fragen mit den staatlichen Datenschutzaufsichtsbehörden statt, um eine gemeinsame Haltung zu den hierbei angesprochenen datenschutzrechtlichen Grundfragen zu gewinnen. Der Beauftragte für den Datenschutz bei der Landeszentrale war in diesem Zusammenhang auch in die Erarbeitung der vom Düsseldorfer Kreis letztlich herausgegebenen "Orientierungshilfe zu Datenschutzanforderungen an Smart-TV Dienste"[120] eingebunden.

Diese Orientierungshilfe informiert über das Thema und die dabei zu beachtenden datenschutzrechtlichen Fragen wie auch über die dazu bestehende Haltung der staatlichen Datenschutzaufsicht; zudem fand aber auch mit einigen Anbietern ein intensiver bilateraler Gedankenaustausch statt. Schließlich wurde das interessierte Publikum auch im Rahmen von Informationsveranstaltungen und über Vorträge informiert.

5.4 Zusammenarbeit von Anbietern mit Social Media-Angeboten

Über Beschwerden wurde die Landeszentrale darauf aufmerksam gemacht, dass einzelne Anbieter im Rahmen von Kooperationen mit Social Media-Anbietern personenbezogene Daten aus dem jeweiligen eigenen Nutzungsverhältnis an die in den USA ansässigen Social Media-Anbieter übermitteln würden. Zu diesem Zweck würden spezielle Produkte eingesetzt und Daten von Email-Adressen von Kunden bis zu Cookie-Informationen, die über das individuelle Nutzungsverhalten Aufschluss gäben, in die USA übersandt.

Tatsächlich existierten wohl zumindest zu bestimmten Zeitpunkten interne Planungen für derartige Zusammenarbeitsformen, die nach heutigem Kenntnisstand aber nie praktisch umgesetzt wurden. Im Übrigen sei es immer nur um die Übermittlung von zusammengefassten und veränderten Daten gegangen, so dass die zu übertragenden Datenbestände keine personenbezogenen Daten enthalten hätten.

Die Frage, ob diese Veränderungsverfahren im konkreten Fall tatsächlich jeden Personenbezug ausgeschlossen hätten, musste abschließend nicht geklärt werden, da die betroffenen Anbieter vor dem Hintergrund der allgemeinen Diskussion über die Frage, ob Hashwerte tatsächlich bzw. unter welchen Voraussetzungen anonym

[120] Stand: September 2015, Version 1.0
abrufbar unter https://www.lda.bayern.de/media/oh_smarttv.pdf

sind und nicht zurückverfolgt werden können, letztlich auf die Umsetzung der Planungen verzichtet haben. Gleichwohl dürften die zugrunde liegenden wirtschaftlichen Überlegungen ebenso wie die sich daran anschließenden datenschutzrechtlichen Fragestellungen für die Zukunft erhalten bleiben.

5.5 Datenpannen

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 sind unterdessen die wesentlichen für den nicht-öffentlichen Bereich maßgeblichen Vorgaben niedergelegt.

Bereits im letzten Berichtszeitraum war eine Datenpanne aufgetreten, die neben persönlichen Daten auch Bank- und Kreditkartendaten betroffen hatte. Wegen des Umfanges wie auch der Bedeutung des Vorgangs, derartige Vorfälle lösen i.d.R. besondere Informationspflichten aus[121], erstreckte sich die Abwicklung und Abarbeitung desselben bis weit in den gegenwärtigen Berichtszeitraum hinein.

Der Beauftragte für den Datenschutz war pflichtgemäß über die Datenpanne informiert worden. Der Anbieter hatte zudem umgehend fachkundige Hilfe von dritter Seite eingeholt, eingehende Nachforschungen angestellt und auch das Cyber Allianz Zentrum Bayern sowie die Strafverfolgungsbehörden eingeschaltet. Insgesamt waren umfangreiche für die Zukunft wirkende präventive, wie auch in die Vergangenheit gerichtete repressive Maßnahmen ergriffen worden. Die maßgeblichen Verfahren dauern zum Teil noch an.

Daneben trat die Prüfung durch den Beauftragten für den Datenschutz bei der Landeszentrale, die sich insbesondere auf die Fragen erstreckte, woher das Datenleck rührte, wie sich der unberechtigte Zugriff ereignete, auf welchen Zeitraum er entfiel, welches Ausmaß er annahm und ob den erforderlichen Benachrichtigungspflichten des Anbieters hinsichtlich der betroffenen Kunden genügt wurde. Weiterhin war sicherzustellen, dass ausreichende technische und organisatorische Maßnahmen die erforderliche Sicherheit für die Zukunft gewährleisten.

Zudem war auch eine erhebliche Anzahl von durch diesen Vorfall ausgelösten Datenschutzbeschwerden, die sich vom vorherigen in den aktuellen Berichtszeitraum erstreckten, zu bearbeiten. Zahlreiche Beschwerdeführer fühlten sich gerade im Hinblick auf die betroffenen Bank- und Kreditkartendaten erheblich verunsichert. Der sich so ergebende unmittelbare Kontakt zu Betroffenen erwies sich für beide Seiten als ebenso nützlich wie in der Sache dienlich.

[121] Vgl. § 15a TMG bzw. § 42a BDSG.

Im aktuellen Berichtszeitraum ereigneten sich weitere Datenpannen i.S.d. § 42a BDSG. Eine solche beruhte auf der Fehlleitung von Mitteilungen, die bedauerlicherweise auch Bankverbindungsdaten umfassten. Insoweit scheint es sich um menschliches Versagen gehandelt zu haben. Möglicherweise war dieses durch die Form der Programmierung eines internen Vorganges erleichtert worden.

Ein anderer Fall betraf von einem Anbieter im Rahmen seines Internetauftritts gesammelte Daten, die zumeist als personenbezogen einzustufen waren. Zu einem geringen Anteil waren auch sensible Daten, wie z.B. Bank- und Finanzdaten betroffen.

Der Beauftragte für den Datenschutz bei der Landeszentrale war in allen Fällen umgehend unterrichtet worden. Auch die weiteren gesetzlich vorgesehenen Formalien wurden eingehalten. Die Datenlecks konnten binnen weniger Tage nach ihrer Entdeckung geschlossen werden. Weitere sichernde Maßnahmen wurden im Nachgang erörtert und zeitnah ergriffen. Zudem wurden auch die Betroffenen innerhalb kurzer Zeit über den Vorgang informiert. Weitere präventive technische und strukturelle Maßnahmen werden geprüft.

5.6 Rundschreiben an Anbieter

Da die die Anbieter betreffenden datenschutzrechtlichen Fragestellungen insgesamt stetig umfangreicher und gelegentlich auch brisanter werden, erscheint es sinnvoll, über aktuelle Entwickelungen von Zeit zu Zeit bei entsprechendem Anlass auch in der Form von Rundschreiben zu informieren.

Besonders hilfreich sind in diesem Zusammenhang häufig die vom Düsseldorfer Kreis[122] herausgegebenen länderübergreifende Orientierungshilfen. Diese Orientierungshilfen geben einen unter den staatlichen Datenschutzaufsichtsbehörden abgestimmten Meinungsstand zu bestimmten Fragestellungen wieder, so dass ihnen daher für die praktische Datenschutzanwendung eine erhebliche Bedeutung zukommt.

Sofern die behandelten Themen auch Fragen des Rundfunks einschließlich der Telemedien betreffen bzw. berühren, wurde in der Vergangenheit häufig auch eine Abstimmung mit dem Beauftragten für den Datenschutz bei der Landeszentrale gesucht, so dass über diese Abstimmungsprozesse auch rundfunkrechtliche Sichtweisen Eingang in die Grundüberlegungen fanden. Insofern eigenen sich diese Orientierungshilfen auch in besonderem Maße zur Information und Sensibilisierung von Rundfunkanbietern im Hinblick auf bei ihnen berührte Datenschutzbelange.

[122] Der Düsseldorfer Kreis dient als Gremium in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder der Kommunikation, Kooperation und Koordinierung der Aufsichtsbehörden im nicht-öffentlichen Bereich.

5.6.1 Rundschreiben zum Positionspapier "smartes Fernsehen nur mit smartem Datenschutz"

Die neueren auch als Smart-TV bezeicheneten Fernsehgeräte bieten neben dem Empfang von Fernsehprogrammen auch die Möglichkeit, Internet-Dienste aufzurufen. Damit ist es z.B. möglich, simultan zum laufenden TV-Programm zusätzliche Web-Inhalte durch die Sender auf dem Bildschirm anzeigen zu lassen. Es ist aber auch umgekehrt möglich, Informationen über das Nutzungsverhalten der Rezipienten zu erhalten, zu speichern und auszuwerten. Von diesen technischen Möglichkeiten internetfähiger TV-Geräte macht eine Reihe von Fernsehanbietern bereits Gebrauch.

Zu den sich hieraus ergebenden datenschutzrechtlichen Fragen hat der Düsseldorfer Kreis unter Beteiligung der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten ein erstes Positionspapier "smartes Fernsehen nur mit smartem Datenschutz" im Jahre 2014 verabschiedet. Diese gemeinsame Position wurde auch von der Konferenz der Direktoren der Landesmedienanstalten politisch unterstützt. Der Beauftragte für den Datenschutz bei der Landeszentrale war an der Abfassung dieses Papiers ebenfalls beteiligt und trägt die gemeinsame Position inhaltlich ebenfalls mit.

Auch wenn dieses Positionspapier letztlich nur einen Zwischenschritt auf dem Wege zu einer endgültigen Haltung der Datenschutzaufsicht bildete, eignete es sich doch sehr gut dazu, die von dieser technologischen Entwicklung und den sich daraus ergebenden Einsatzmöglichkeiten berührten datenschutzrechtlichen Fragen und Problemstellungen darzustellen. Aus diesem Grunde wurden alle Geschäftsführer der von der Landeszentrale genehmigten TV-Anbieter mit einem Rundschreiben vom 23.07.2014 über den Inhalt des Positionspapiers unterrichtet.[123]

5.6.2 Rundschreiben zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter

Nachdem die Präsenz privater Rundfunkanbieter im Zuge des Wandels der Mediennutzung inzwischen im Internet selbstverständlich ist, werden Apps heute in unterschiedlicher Form und mit vielseitigen Zielsetzungen auch von Rundfunkanbietern eingesetzt. Hierbei ist zu beachten, dass der App-Anbieter gegenüber den Mediennutzenden in der Regel eine datenschutzrechtliche Verantwortung trägt und die entsprechenden Datenschutzvorgaben zu erfüllen hat.

Das Bayerische Landesamt für Datenschutzaufsicht in Ansbach hat inzwischen bereits das zweite Mal Apps bayerischer Unternehmen überprüft und

[123] Vgl. zu dieser Problematik oben 5.2

ist zu dem Ergebnis gekommen, dass die schlechte datenschutzrechtliche Bewertung insbesondere der bayerischen iOS-Apps zeige, dass die datenschutzrechtlichen Anforderungen durch bayerische App-Anbieter noch nicht ausreichend wahrgenommen würden. Da die Feststellungen des Landesamts für Datenschutzaufsicht darauf schließen lassen, dass auch im Bereich des privaten Rundfunks noch Nachbesserungsbedarf besteht, informierte der Beauftragte für den Datenschutz alle bei der Landeszentrale genehmigten Hörfunk- und Fernsehanbieter sowie ihre Verbände mit einem Rundschreiben vom 17.12.2015 über die von App–Entwicklern und App–Anbietern zu beachtende datenschutzrechtliche Gesichtspunkte. Die Basis hierfür bildete eine Orientierungshilfe des Düsseldorfer Kreises zu diesem Thema.[124].

Diese Orientierungshilfe konkretisiert die rechtlichen und technischen Rahmenbedingungen, die sich aus dem Telemedien- bzw. Bundesdatenschutzgesetz ergeben. Sie enthält grundsätzliche Hinweise für das Erstellen und Verwenden von Apps, insbesondere über den Inhalt und den Umfang zulässiger Datenerhebungen, die dabei zu beachtenden Zweckbindungen, die geltenden Verantwortlichkeiten und einzuhaltenden Sicherheits- und Schutzmechanismen. Im Zentrum stehen naturgemäß die Anforderungen für den Umgang mit den bei der App-Nutzung anfallenden Daten bis hin zur Datenübermittlung in Drittstaaten. Aber auch zu den Themen Anmeldedaten, eindeutige Kennung, sichere Datenübertragung, lokale Datenspeicherung oder Nutzung von App-Stores werden zutreffende Hinweise gegeben.
Ungeachtet der bestehenden besonderen rundfunkrechtlichen Zuständigkeiten erscheint eine Kenntnis der in dieser Orientierungshilfe niedergelegten Auffassungen auch deswegen als wichtig, da die Tätigkeit der App-Entwicklung ihren Anwendungsbereich sowohl innerhalb wie außerhalb des Rundfunks hat. Zudem werden die in dieser Orientierungshilfe vertretenen Auffassungen weitestgehend geteilt, so dass sich eine möglichst frühzeitige Beachtung oder jedenfalls Kenntnis dieser Auffassungen auch angesichts der Überschneidungen der Zuständigkeiten empfiehlt.

6. Weiterbildung

Die kontinuierliche Weiterbildung 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 hierbei insbesondere der Sitzungen des Erfa-Kreises Bayern, in denen einerseits ausgewählte Institutionen und Firmen in Vorträgen und Erfahrungsberichten ihre besonderen Aufgabenschwerpunkte und die dabei zu beachtenden und zu bewältigenden datenschutzrechtli-

[124] Orientierungshilfe zu den Datenschutzanforderungen an die App–Entwickler und App–Anbieter
Stand: 16. Juni 2014 abrufbar unter: https://www.lda.bayern.de/media/oh_apps.pdf

chen Herausforderungen vor- und zur Diskussion stellen. Andererseits werden in diesen Veranstaltungen auch allgemeine und spezielle datenschutzrechtliche Fragestellungen erörtert, von fachkundiger Seite über die aktuelle Rechtsentwicklung berichtet und diese fachlich bewertet.

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 und 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; beispielhaft sei eine solche zum Thema "Schuldfrage bei Datenverlust" im Bayerischen Landeskriminalamt genannt.

Darüber hinaus wird ein laufender Erfahrungsaustausch mit dem Bayerischen Landesamt für Datenschutzaufsicht in Ansbach und werden Kontakte zum Landesbeauftragten für den Datenschutz wie auch zum für Datenschutzrecht zuständigen Referat des Innenministeriums 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 bereithält. Dies gilt insbesondere für die Institution des Rundfunkdatenschutzbeauftragten, 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 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 aber auch in Bayern konsequent fortentwickelt werden sollte.

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 Plattformen, zu denen ggf. künftig auch Intermediäre gehören könnten, ebenso wie für die oben dargestellten Entwicklungen unter den Stichworten Smart-TV und HbbTV, die wegen ihrer intensiven rundfunkrechtlichen Bedeutung einer Lösung bedürfen, die Besonderheiten des Rundfunkrechtes aufnimmt und ihnen gerecht wird.