Bayerische Landeszentrale für neue Medien

Zehnter Tätigkeitsbericht
des Beauftragten für den Datenschutz
bei der Bayerischen Landeszentrale für neue Medien
(Berichtszeitraum: 01.01.2010 bis 31.12.2011)

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 zehnte Tätigkeitsbericht seit Inkrafttreten des BayMG am 01.12.1992 und bezieht sich auf die Jahre 2010 und 2011.

Der Schwerpunkt meiner Tätigkeit lag im Berichtzeitraum neben der Beratung von Landeszentrale und Anbietern hinsichtlich der 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.

Förmliche Beanstandungen musste ich im Berichtzeitraum nicht aussprechen.

2. Entwicklung des Datenschutzrechts

2.1 Internationale Entwicklungen

Aufgrund der stetig wachsenden Internationalisierung der Weltwirtschaft wie auch der weltweiten Arbeitsteilung gewinnt der weltweite Datenaustausch immer mehr an Bedeutung, so dass es sinnvoll erscheint, auch diese Entwicklungen zu beachten und über sie zu berichten.

2.1.1 Beschluss des Düsseldorfer Kreises vom 29.04.2010 zum 10-jähigen Bestehen des „Safe-Habor"-Abkommens

Das zum 26.07.2000 abgeschlossen Safe-Habor Abkommen wurde von der Europäischen Union und den Vereinigten Staaten geschlossen, um den Datentransfer in die USA hohen Sicherheitsstandards zu unterwerfen.

Die Regelung für den Internationalen Datentransfer findet sich in § 4 b BDSG. Danach dürfen personenbezogene Daten nicht in das außereuropäische Ausland übermittelt werden, soweit der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn beim Empfänger ein angemessenes Datenschutzniveau nicht gewährleistet ist, § 4 Abs. 2 Satz 2 BDSG. Nach der Europäischen Datenschutzrichtlinie 95/46/EG (im Folgenden EU-DSRL) kann die Kommission feststellen, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen ein angemessenes Schutzniveau gewährleistet, vgl. Art. 25 Abs. 2 i. V. m. 26 Abs. 2 u. 4 i. V. m 31 Abs. 2 EU-DSRL.

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 gelten die Safe Habor Priciples[1], die von der EG-Kommission am 26.07.2000 entschieden und seit November 2000 praktiziert werden.

Amerikanische Unternehmen schaffen die Voraussetzung für den Datentransfer mit angemessenem Schutzniveau von Europa aus, indem sie sich selbst zertifizieren. Dies erfolgt, indem sich die Unternehmen auf die Grundsätze der Safe Habor-Vereinbarung verpflichten und eine Meldung an die Federal Trade Comission (FTC) abgeben. Im Internet findet sich die Safe Habor-Liste, die vom US-Handelsministerium veröffentlicht wird.[2]

In einer Studie zum Safe Habor Treatment von 2008[3] wird die Einhaltung des Abkommens untersucht und u. a. kritisiert, dass von der angegebenen Zahl von 1700 Organisationen, die nach Safe Habor zertifiziert sind, nur 348 den Kriterien des Abkommens entsprechen[4]. Auch der Düsseldorfer Kreis, ein Zusammenschluss der obersten Datenschutzaufsichtsbehörden für den nichtöffentlichen Bereich, hat Ähnliches festgestellt. Diese Diskussion ist von Bedeutung, da große Netzwerke wie Google und Facebook in Deutschland erhobene Daten in den USA verarbeiten lassen. Deren Datenschutzbestimmungen verweisen auf das Safe-Habor Abkommen und der nichtinformierte Leser meint, seine personenbezogenen Daten seien dort in guten Händen, z.B. weil bei Facebook die TRUSTe die Datenschutzrichtlinien geprüft und genehmigt habe; tatsächlich aber ist TRUSTe ein von Facebook finanziertes Zertifizierungsunternehmen.[5]

Der Düsseldorfer Kreis hat daraufhin am 29.04.2010 u.a. beschlossen: „Solange eine flächendeckende Kontrolle der Selbstzertifizierung US-amerikanischer Unternehmen durch die Kontrollbehörden in Europa und den USA nicht gewährleistet ist, trifft auch die Unternehmen in Deutschland eine Verpflichtung, gewisse Mindestkriterien zu prüfen, bevor sie personenbezogene Daten an ein auf der Safe Habor-Liste geführtes Unternehmen übermitteln".[6]

[1] http://export.gov/safeharbor/eu/eg_main_018365.asp
[2] http://safehabor.export.gov/list.aspx
[3] Conolly, The US Safe Habor – Fact or Fiction? (2008), www.galexia.com
[4] Erd, Safe Habor Abkommen in K&R S. 626
[5] Erd, o.a.a S. 627
[6] Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 28./29.04.2010 in Hannover, S.1

Die exportierenden Unternehmen müssen sich somit vergewissern, ob die Safe-Habor-Selbstzertifizierung des importierenden Unternehmens noch gültig ist. Es muss sich zudem nachweisen lassen, wie dieses seinen Informationspflichten nach Safe Habor gegenüber den von der Datenverarbeitung Betroffenen nachkommt[7]. Diese Mindestprüfung muss das exportierende Unternehmen dokumentieren und auf Nachfrage der Aufsichtsbehörde nachweisen[8]. Sofern sich nach Prüfung Zweifel ergeben sollten, empfehlen die Aufsichtsbehörden, die Verwendung von Standard-Vertragsklauseln oder bindenden Unternehmensrichtlinien zur Gewährleistung eines angemessenen Datenschutzniveaus.[9] Ggf. sollte die zuständige Datenschutzaufsicht informiert werden.

2.1.2 Gesetzesvorhaben in den USA (SOPA und PIPA[10])

SOPA (Stop Online Piracy Act)[11] ist ein Gesetzesentwurf vom 26. Oktober 2011, der im US-amerikanischen Repräsentantenhaus vom Abgeordneten Lamar Smith (Republikanische Partei Texas) eingebracht wurde, und steht für eine ganze Reihe ähnlicher Vorgänge, die grundlegende Bedeutung für die weltweit geltenden Regeln im Internet haben könnten. SOPA baut auf PIPA (PROTECT IP act) und damit Gesetze bzw. Gesetzesvorhaben aus den Jahren 2008 und 2011 auf. Das SOPA-Gesetzgebungsverfahren ist nach heftigen weltweiten Protesten, wie etwa am 18. Januar 2012 das Abschalten von Wikipedia für 24 Stunden oder die 3,3 Mio gesammelten Internetunterschriften von Aavaz, derzeit zum Erliegen gekommen.

Dieses Gesetz soll es Urheberrechtsinhabern ermöglichen, die nicht genehmigte Verbreitung urheberrechtlich geschützter Inhalte wirksam zu verhindern. Es soll dem US-Justizminister und Urheberrechtsinhabern erlauben, gerichtliche Verfügungen gegen Internetseiten zu beantragen, welche einen Verstoß gegen das US-amerikanische Urheberecht darstellen. Dabei könnte der Zweck und Inhalt der Maßnahme vom Antragsteller gewählt werden, wie z.B. das Anzeigen der betroffenen Internetseite in Suchmaschinen zu blockieren.

Befürworter sind der Ansicht, das Gesetz diene dem Schutz des geistigen Eigentums und würde damit verbundene Arbeitsplätze und Firmen schützen.

[7] Beschl. der obersten Aufsichtsbehörden a.a.O., S.1
[8] Beschl. der obersten Aufsichtsbehörden a.a.O., S.2
[9] a.a.O. Fn. 7
[10] Quelle: http://de.wikipedia.org/wiki/Stop_Online_Privacy_Act
[11] Bill Text, 112th Congress (2011-2012), H.R.3261.IH

Die Gegner wie z.B. auch Google, Yahoo, Facebook, Ebay sowie Bürgerrechtler und Journalisten halten den Gesetzesentwurf für Zensur. Es würde das Internet knebeln und überdies verstoße es gegen das Recht auf Meinungsfreiheit.[12]

Auch PIPA („Protect IP Act"), ein von den Demokraten im Senat eingebrachter Gesetzesvorschlag, sah im Kampf gegen Raubkopien Netzsperren vor. Gegner waren auch dort der Ansicht, dass dies die offene Struktur des Internets gefährde. Missliebige Inhalte könnten zensiert und Internetnutzer schikaniert werden. Insgesamt seien die Protestierenden nicht für weniger Urheberrechtsschutz, jedoch halte man die Vorlagen für ungeeignet.
Aufgrund der vorgenannten weltweiten Proteste wurde die für den 24. Januar 2012 geplante Abstimmung über das Gesetzesvorhaben PIPA verschoben.

2.1.3 ACTA – Anti-Counterfeiting Trade Agreement vom 03.12.2010

Das ACTA-Abkommen[13], das auch „Anti-Piraterie-Abkommen" genannt wurde, war als ein multilaterales Handelsabkommen auf völkerrechtlicher Ebene geplant, um internationale Standards im Kampf gegen die Produktpiraterie und Urheberrechtsverletzungen zu schaffen. Am 16.12.2011 hat der EU-Rat dem Handelsabkommen seine Zustimmung gegeben. Am 26.01.2012 hatten nach Kanada, Australien, Japan, Marokko, Neuseeland, Südkorea, Singapur und den USA bereits auch 22 der 27 EU-Mitgliedstaaten das Abkommen unterzeichnet. Die EU hatte zudem bereits für ihre Mitgliedstaaten unterzeichnet. Deutschland hatte aus formalen Gründen noch nicht selbständig unterschrieben, eine Unterschrift war offenbar aber angekündigt.

Der Vertrag soll den Schutz des geistigen Eigentums und der Urheberrechte im Internet stärken. Die über drei Jahre andauernden Verhandlungen, in der die EU-Mitgliedstaaten durch die Europäische Kommission vertreten wurden, fanden erst im Geheimen statt. Nach Protesten von Bürgerrechtlern wurde im April 2010 eine umfassende Dokumentation auf der Internetseite der Kommission zur Verfügung gestellt[14]. Nach diesen Informationen sollten keine Internetseiten geschlossen werden können. Es ginge nur um die Bekämpfung organisierter Kriminalität von geistigem Eigentum und nicht darum die täglichen Nutzungsgewohnheiten im Internet zu beschränken. Die Nutzung sozialer Netzwerke wie Twitter und Facebook solle sich nicht ändern.

[12] Siehe Fn. 10
[13] Rat der Europäischen Union, institutionelles Dossier: 2011/0166 (NLE), letzter Stand vom 09. September 2011, 12196/3/11 REV 3 (de)
[14] http://ec.europa.eu/trade/creating-opportunities/trade-topics/intellectual-property/anti-counterfeiting/

Es würden weder Computer, iPads oder iPhones überprüft werden, ACTA sei nicht Big Brother. ACTA mache keine EU Gesetzesänderungen erforderlich. Alles was bisher legal sei, wäre auch nach der Ratifizierung noch legal.[15]

Der Bundesbeauftragte für Datenschutz und Informationsfreiheit teilt in seinem Tätigkeitsbericht 2009/2010[16] mit, dass bei der Beratung des Abkommens unter anderem davon die Rede gewesen sei, die Anbieter von TK-Leistungen darauf zu verpflichten, die Kunden mit Blick auf Verstöße etwa gegen Urheberrecht zu überwachen. Bei der Verletzung der Überwachungspflichten sei eine Haftung der Provider für evtl. Verstöße der Nutzer angedacht gewesen. Da bei der Überwachung die Kundendaten gespeichert werden müssten, würde dies als Vorratsdatenspeicherung und damit als unzulässig angesehen, da es sich um eine anlasslose Speicherung von IP-Adressen und TK-Verkehrsdaten handeln würde. Die entsprechenden Regelungen seien aber nicht in den Vertragstext aufgenommen worden.

Die Bundesregierung war der Ansicht, das Vertragswerk ACTA sei „notwendig und richtig".[17] Bundesjustizministerin Sabine Leutheusser-Schnarrenberger lehnt die Unterschrift ab, da sie die Entscheidung des EU-Parlaments abwarten wollte.

Stimmen aus der Wirtschaft[18] äußerten sich im Gegensatz dazu dahin, dass nach den Intentionen der Inhaber der Urheberrechte Internetprovider nur dann haftungsfrei bleiben sollten, wenn sie die komplette Kommunikation der Nutzer überwachten. Die Urheberrechtsverstöße sollten dann direkt vom Provider gegenüber dem Nutzer geahndet werden, d.h. von der Verwarnung bis hin zur Kündigung des Internetanschlusses. Kritisiert wurde hierbei, dass alles ohne staatliches Verfahren abgewickelt würde, obgleich eine Kündigung für manche Selbständige heutzutage einem Berufsverbot gleichkomme. Die Unterzeichnung des Abkommens sei ein Akt weg von der Rechtsstaatlichkeit hin zur Zensur, Überwachung und Strafen ohne gerichtliches Verfahren.

Nach einer reichhaltigen öffentlichen Diskussion wurde schließlich das Abkommen im Europaparlament abgelehnt. Nachdem auch die EU-Kommission ihre diesen Vorgang betreffende Anfrage beim EuGH zurückgezogen hat, dürfte das Abkommen zumindest derzeit keine Chance auf Verwirklichung in Europa haben.

[15] Siehe Fn. 14
[16] Tätigkeitsbericht des Bundesbeauftragten für Datenschutz und Informationsfreiheit 2009/2010, S. 52
[17] www.zeit.de/digital/internet/2012-07/eu-parlament-lehnt-acta-ab
[18] Bericht im Handelsblatt vom 25.01.2012

2.2 Europäisches Recht

Das nationale Datenschutzrecht ist zunehmend durch Vorgaben der Europäischen Union geprägt. Den grundlegenden Rahmen geben bisher die EU-Datenschutzrichtlinie[19] sowie die E-Privacy-Richtlinie (RL 2002/58/EG)[20] vor, die die Harmonisierung der sich aus dem Datenschutz ergebenden Anforderungen im Hinblick auf einen einheitlichen Wirtschaftsrahmen als Ziel verfolgen.

2.2.1 Der Vertrag von Lissabon

Der Vertrag von Lissabon, der am 13. Dezember 2007 von den europäischen Staats- und Regierungschefs unterzeichnet worden ist, bringt nach dem Inkrafttreten am 1. Dezember 2009 maßgebliche Änderungen für den Datenschutz. Durch den Vertrag von Lissabon werden die bislang geltenden Gemeinschaftsverträge grundlegend umgestaltet. Eine entscheidende Neuerung ist die Aufhebung der Säulenstruktur[21] und die Einbindung der Charta der Grundrechte in das europäische Primärrecht. Für den datenschutzrechtlichen Bereich ergeben sich daraus folgende Änderungen:

- Gem. Art. 16 Abs. 2 AEUV[22] verpflichten sich die europäischen Gesetzgebungsorgane zum Erlass von Datenschutzvorschriften; die Einhaltung dieser Vorschriften soll von unabhängigen Behörden überwacht werden. Diese Verpflichtung gilt nicht nur für die Verarbeitung personenbezogener Daten durch europäische Institutionen, sondern nunmehr auch für die Verarbeitung von Daten durch die Mitgliedsstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Unionsrecht fallen. Inzwischen liegt ein Entwurf einer Datenschutzgrundverordnung[23] vor, welche die EU- Datenschutzrichtlinie (95/46/EG) ablösen soll.

- Mit dem Wegfall der bisherigen Säulenstruktur wird der bisher der dritten Säule zugehörende Bereich der zwischenstaatlichen polizeilichen- und justiziellen Zusammenarbeit „vergemeinschaftet“ und unterliegt nunmehr grundsätzlich auch dem Geltungsbereich des Art. 16 AEUV.

[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] 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).
[22] Vertrag über die Arbeitsweise der Europäischen Union.
[23] Vgl. unten 2.2.2

Am 27. November 2008 hat der Rat der EU-Innen- und Justizminister einen Rahmenbeschluss über den Datenschutz in der dritten Säule verabschiedet.[24] Es erscheint jedoch zweifelhaft, ob dieser den Anforderungen des Art. 16 AEUV entspricht. Problematisch ist insbesondere, dass der Rahmenbeschluss sich nur auf die grenzüberschreitende Kommunikation und nicht auf die Datenverarbeitung in den Mitgliedsstaaten selbst bezieht, obwohl die übermittelten Daten im Empfängerland mit den dort erhobenen Daten zusammengeführt werden. Als unbefriedigend wird der Beschluss auch hinsichtlich des Rechtes des Betroffenen auf Auskunft empfunden, weil die konkrete Ausgestaltung den Mitgliedsstaaten überlassen wurde. Parallel zum Entwurf der Datenschutzgrundverordnung wurde daher der Vorschlag einer Richtlinie[25] zur Harmonisierung des bisher im Rahmenbeschluss 2008/977/JAH regulierten Bereiches vorgelegt.

- Die wohl wichtigste Änderung ist jedoch die Bezugnahme auf die Charta der Grundrechte im Vertrag von Lissabon. In Art. 8 der Grundrechtecharta ist ein Grundrecht auf Datenschutz normiert, das zum ersten Mal auf europäischer Ebene rechtsverbindlich ist. Das bewährte Grundrecht auf informationelle Selbstbestimmung darf durch europäische Regelungen zwar ergänzt, aber nicht verdrängt werden, da die europäischen Grundrechte noch kein vergleichbares Schutzniveau gewährleisten.[26]

- Da inzwischen der Entwurf für eine EU-Verordnung, die sog. Datenschutz-Grundverordnung, sowie die vorgenannte Richtlinie im Bereich der Strafjustiz und – vollstreckung vorliegen, wird auch die gegenteilige Auffassung vertreten. In diesem Zusammenhang vertritt der (voraussichtlich im maßgeblichen Senat auch inhaltlich zuständige) Bundesverfassungsrichter Prof. Masing[27] in einer öffentlichen Stellungnahme die Auffassung, dass mit einer solchen Verordnung als unmittelbar geltendem europäischem Recht sogar deutsches Verfassungsrecht verdrängt würde und damit nicht nur Folgewirkungen für den Datenschutz in Deutschland, sondern auch auf das Verfassungsrecht bis hin zur Geltung des bisherigen Grundrechtsschutzes verbunden seien.

[24] ABl. EU 2008/L 350/60.
[25] „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr“, vgl. KOM(2012) 10 **endg.**
[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

2.2.2 EU-Datenschutz-Grundverordnung

2.2.2.1 Allgemeines

Bereits am 6. Dezember 2011 wurde der erste inoffizielle Entwurf der geplanten „Datenschutz-Grundverordnung" im Internet veröffentlicht.[28]

Am 25. Januar 2012 hat Frau Kommissarin Redding den Entwurf einer europäischen Datenschutz-Grundverordnung[29] vorgelegt, der in verschiedener Hinsicht einen Meilenstein darstellen soll, sofern diese Verordnung geltendes Recht werden sollte. Der Verordnungsentwurf wurde auch im Vorfeld bereits intensiv diskutiert.

Zentrales Anliegen dieser Verordnung ist es, einerseits einen einheitlichen europäischen Datenschutzstandard verbindlich für das gesamte Gebiet der Europäischen Union vorzugeben, der auf diese Art und Weise die unterschiedlichen Datenschutzniveaus in den 27 Mitgliedsstaaten angleichen würde. Andererseits soll die Verordnung die Bedeutung des europäischen Datenschutzes dadurch erheblich erhöhen, dass diese Regeln auch für außereuropäische Stellen gelten sollen, sofern diese Stellen Datenverarbeitungsvorgänge in Bezug auf das EU-Inland vornehmen oder damit das Verhalten von Einwohnern der EU überwachen könnten.

Insofern hofft man, ein derartiger einheitlicher Rechtsrahmen würde den Wettbewerb gerade zwischen solchen Unternehmen deutlich befördern, die für ihre Geschäftsmodelle einer entsprechenden Datenverarbeitung bedürfen oder gar diese Daten ins Zentrum ihres Geschäftsmodells stellen. Zudem sollen so die bisher beklagten Unterschiedlichkeiten der Datenschutzanforderungen der 27 EU-Staaten beseitigt und für eine größere Wettbewerbsgleichheit zwischen europäischen und außereuropäischen Unternehmen auf dem europäischen Markt gesorgt werden.

Die gewählte Methode einer europäischen Verordnung würde einen unmittelbar in allen Mitgliedsstaaten der EU anzuwendenden Rechtsbestand schaffen, der als europäisches Recht nationalem Recht vorgehen und dieses verdrängen würde.

---

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

[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) – vom 25.01.2012, KOM (2012) / 11 endgültig*

Dies würde den oben geschilderten Zielen entsprechen, würde aber auch die Unterschiedlichkeiten in der bisher gekannten nationalen Ausgestaltung einebnen, was Auswirkungen bis zu den bisher grundrechtliche garantierten Ansprüchen auf informationelle Selbstbestimmung bzw. auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme haben könnte. Wie bereits erwähnt vertritt sogar der Bundesverfassungsrichter Prof. Masing[30] die Auffassung, dass eine solche Verordnung als unmittelbar geltendes europäisches Recht sogar deutsches Verfassungsrecht verdrängen würde.

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, bildet andererseits aber auch einen Kernpunkt der Kritik, die dies für eine unausgewogene Überbetonung des Individualdaten- und des Persönlichkeitsrechtschutzes hält. Dies führe für die Internetwirtschaft zu vollkommen unpraktikablen Bedingungen, da der Massenverkehr im Internet standardisierte vorformulierte Einwilligungserklärungen erforderlich mache, und daher das stetige Gebot der Einwilligung entweder zu einem inhaltsleeren Automatismus führen würde, oder aber die Internetwirtschaft in zentralen Punkten massiv behindert würde.

Zudem würden die entgegen stehenden Rechte Dritter wie z.B. Kommunikationsfreiheiten nicht in ausreichendem Maße berücksichtigt. Das deutsche Recht sehe mit guten Gründen daher stets eine entsprechende Interessenabwägung vor. Gelegentlich wird gar eingewandt, diese Überbetonung des Individualrechtschutzes sei verfassungswidrig. Hierauf dürfte es allerdings nicht mehr ankommen, da die nationalen Grundrechte bei einer EU-Verordnung gerade als Korrektiv ausscheiden dürften. Allenfalls könnte ein Verstoß gegen europäische Grundrechte vorliegen, der beim EuGH zu rügen wäre. Dass es dort keine dem BVerfG entsprechende Expertise in Sachen Grundrechtsschutz gibt, wäre dann ein Umstand, an den man sich gewöhnen müsste.

Zudem wird der Datenschutz-Grundverordnung vorgeworfen, dass sie ungerechtfertigter Weise alle Daten gleich behandele, während die Rechtsbetroffenheit des Einzelnen je nach Inhalt des jeweiligen Datensatzes deutlich unterschiedlich ausgestaltet sei. Gegen diese Kritik ist jedoch einzuwenden,

[30] Johannes Masing, „Ein ‚Abschied von den Grundrechten“, SZ 29.01.2012

dass die Bedeutung von personenbezogenen Daten in der heutigen Zeit nie losgelöst vom jeweiligen Einsatz der Datenverarbeitung im Einzelfall beurteilt werden kann und die individuelle Nutzungssituation vorab wohl kaum so einschätzbar sein dürfte, dass eine genau Klassifizierung der Inhalte der betroffenen Daten möglich wäre. Vielmehr kann eine Abwägung zwischen betroffenen Rechtspositionen stets nur im Einzelfall und unter Einbeziehung des konkreten Nutzungszusammenhangs getroffen werden. Das deutsche Datenschutzrecht kennt daher auch nur eine Hervorhebung von Daten als besonders sensibel[31]; dies betrifft solche über rassische oder ethnische Herkunft, politische Meinungen, religiöse oder ethische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben. Im Übrigen findet i.d.R. eine Klassifizierung nicht statt.

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, das den ursprünglich die Daten verarbeitenden Unternehmen aufgibt, für die Löschung auch in anderen öffentlich zugänglichen Kommunikationsdiensten namentlich Suchdiensten zu sorgen. Für die Praxis geht man wohl nahezu einhellig davon aus, dass dies nicht umsetzbar sein und daher nur einen qualifizierten Löschungsanspruch darstellen wird.

Zudem soll es dem Einzelnen ermöglicht werden, die über ihn gespeicherten Daten auch in gesammelter Form von einem Internetanbieter abzuziehen, um mit diesen Daten den Anbieter für ein bestimmtes Angebot zu wechseln, was den Wettbewerb zwischen konkurrierenden Anbietern deutlich verbessern würde, jedoch wohl kaum gleichermaßen von allen Marktteilnehmern begrüßt wird. Unterdessen bestehen erhebliche Zweifel an den Chancen der technischen Umsetzung, die ein einheitliches Datenformat voraussetzen dürfte, das jedenfalls noch nicht existiert.

Daneben gibt es aber auch weitere kritische Stimmen, die insbesondere darauf hinweisen, dass mit der Datenschutz-Grundverordnung erhebliche neue Kompetenzen auf die europäische Ebene gezogen würden. Dies gilt insbesondere für Kompetenzen und Zuständigkeiten für ausgestaltende gesetzgeberische sowie administrative Tätigkeiten. Die Datenschutz-Grundverordnung sieht für 26 Artikel die Zuständigkeit der EU-Kommission für Delegierte Rechtsakte vor, so dass die Kommission in diesen Materien die Befugnis zum

[31] Vgl. § 3 Abs. 9 BDSG

Erlass von Vorschriften erhalten würde, die die zumeist allgemein gehaltenen Vorgaben der Datenschutz-Grundverordnung als europäischer Gesetzgeber konkretisieren. Die erlassenen Rechtsakte würden wirksam, sofern das EU-Parlament nicht innerhalb von zwei Monaten Einwände erhebt.

Die Datenschutz-Grundverordnung regelt in Art. 89 das Verhältnis zur Richtlinie 2002/58/EG. Danach soll die Datenschutzgrundverordnung für die Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen dann nicht gelten, wenn die Richtlinie 2002/58/EG für diese bereits Pflichten festlegt, die dasselbe Ziel verfolgen. Die Reichweite dieser Bestimmung ist derzeit kaum abzuschätzen, denn Pflichten ergeben sich aus der Richtlinie 2002/58/EG zahlreiche. Da gerade die großen amerikanischen Anbieter wie Google und Facebook zweifellos Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen sein dürften, wäre ein Anwendungsausschluss der Datenschutz-Grundverordnung für diese Angebote sehr bedauerlich und würde die Ziele der Datenschutz-Grundverordnung deutlich berühren.

2.2.2.3 Bewertung des Vorhabens

Die Datenschutz-Grundverordnung hält viele Anreize für zahlreiche Gruppen von Betroffenen bereit. Ob sich alle Vorgaben und Erwartungen werden verwirklichen lassen, erscheint mehr als zweifelhaft. Fraglich ist daher, ob die für die Bürger tatsächlich entstehenden Vorteile insbesondere angesichts der heute schon absehbaren Abstriche gegenüber den ursprünglichen Ankündigungen die mit der Datenschutz-Grundverordnung verbundenen Nachteile wirklich aufwiegen können. Dies gilt insbesondere für die vom Prof. Masing angesprochenen, zu erwartenden Folgewirkungen für die künftige Geltung und Bedeutung des nationalen Verfassungsrechts. Ob eine Verordnung wirklich der vorzugswürdige Weg sein kann, erscheint deshalb durchaus zweifelhaft.

Insofern dürfte eine Umsetzung der inhaltlichen Planungen in der Form einer Richtlinie den besseren weil flexibleren Weg darstellen, der auch den sehr unterschiedlichen Historien in den Mitgliedsstaaten der EU deutlich besser gerecht würde. Ggf. könnte ja auch eine Kombination aus Richtlinie und Verordnung eine Lösung darstellen. Bei dieser würden nur diejenigen Bestandteile der Planungen in einer Verordnung verbindlich unmittelbar vorgeschrieben, die dieser Rechtsqualität unbedingt bedürfen, und die auch mit solcher Klarheit erlassen werden, dass es nicht derart weitgehender Kompetenzen der EU-Kommission zur Konkretisierung bedarf, wie dies derzeit vorgesehen

ist. Die übrigen Materien, bei denen ohnehin noch keine für eine praktikable gesetzliche Regelung hinreichende Klarheit bestehen, könnten in einer Richtlinie niedergelegt werden, bei welchen solche Spielräume üblich sind, und die dann durch nationales Recht umgesetzt und konkretisiert werden könnten, für welche dann aber die nationalen Grundrechte als verbindliche Schranken bestehen blieben.

2.2.3 Urteil des EuGH zur Vorratsdatenspeicherung - aktueller Stand

Mit der Richtlinie 2006/24/EG[32] des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, wurden Eckpunkte für die Vorratsdatenspeicherung festgelegt. Danach müssen die Mitgliedsstaaten dafür Sorge tragen, dass von Anbietern von Telekommunikationsdiensten Verbindungsdaten von mindestens sechs Monaten bis zu höchstens zwei Jahren auf Vorrat gespeichert werden, Art. 3 i.V.m Art. 6 RL. Die Kategorien der zu speichernden Daten sind in Art. 5 RL beschrieben und umfassen etwa bei Telefongesprächen die Telefonnummer, Namen und Anschrift sowie den Zeitpunkt und Dauer des Gesprächs. Bei der Nutzung von Mobilfunkgeräten kommen Funkzelle, Identifikationsnummer und geografische Ortung dazu. Betreffend die Internetnutzung sollen Benutzerkennung und IP-Adressen gespeichert werden und beim E-Mailverkehr werden Kontaktdaten und Zeiten der Internetnutzung gespeichert.

Die gegen diese Richtlinie gerichteten Klagen von Irland und der Slowakei wurden am 10. Februar 2009 vom EuGH mit Urteil[33] zurückgewiesen und entschieden, dass die Richtlinie (2006/24/EG) auf der Grundlage des EG- Vertrages, insbesondere Art. 95 EG, wirksam erlassen wurde. Der EuGH stellte hierbei klar, dass die Entscheidung keinerlei Aussage zu einer möglichen Verletzung der Grundrechte durch die Richtlinie in materieller Hinsicht trifft, sondern sich lediglich auf die richtige Wahl der Rechtsgrundlage bezieht.

Es sei gerechtfertigt, dass der Gemeinschaftsgesetzgeber das Ziel, das Funktionieren des Binnenmarkts zu schützen, durch den Erlass von Harmonisierungsvorschriften verfolgte.[34]

---

[32] ABl. EG v. 15.03.2006, Nr. L 105/54.

[33] EuGH Urt. v. 10.02.2009, Az: C-301/06.

[34] Diese Begründung erscheint vor allem deshalb diskussionswürdig, weil die Richtlinie keineswegs nur Speicherungspflichten harmonisiert, sondern solche Verpflichtungen auch für die Länder verbindlich einführt, in denen es bis dahin keine derartige Verpflichtung gab, und zudem auch berechtigte Zweifel bestanden, ob alle nationalen Gesetzgeber eine solche Verpflichtung einführen könnten, geschweige denn würden. Ebenso erscheint zweifelhaft, ob eine solche Verpflichtung wirklich für das Funktionieren des Binnenmarktes erforderlich ist. Die Richtlinie hat tiefer gehende Auswirkungen auf den realen Datenschutz der Gemeinschaftsbürger

In Deutschland wurde die Richtlinie mit dem „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer versteckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“[35] umgesetzt. Das Gesetz wurde am 09.11.2007 im Bundestag verabschiedet und am 26.12.2007 vom Bundespräsidenten unterzeichnet. Es trat am 01.01.2008 in Kraft. Das Bundesverfassungsgericht hat dieses Gesetz auf seine Vereinbarkeit mit dem Grundgesetz geprüft und mit Urteil vom 02.03.2010 verworfen.[36]

Das Gericht ist 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“.[37]

Aufgrund tief gehender Meinungsverschiedenheiten innerhalb der Bundesregierung ist es bisher zu keiner Neuregelung gekommen[38]. Das Bundesjustizministerium hat am 7.6.2011 einen eigenen Diskussionsentwurf für ein „Gesetz zur Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdaten im Internet“[39] eingebracht. Vorgesehen wird zum einen eine Anordnungsbefugnis der Strafverfolgungsbehörden, mithilfe derer Telekommunikationsunternehmen im Rahmen von Ermittlungsverfahren anlassbezogen verpflichtet werden können, bei diesen vorhandene (d.h. freiwillig gespeicherte) und künftig anfallende Verkehrsdaten kurzfristig vorsorglich zu sichern, um einer Löschung zuvorzukommen und sie einem gegebenenfalls nötig werdenden späteren Abruf zugänglich zu machen (Quick Freeze). Zum anderen würde zum Zwecke der Gewährleistung der in der Praxis wichtigen Bestandsauskünfte im Internet (wer verbirgt sich hinter einer bereits ermittelten IP-Adresse?) eine Art „kleine“ Vorratsdatenspeicherung eingeführt, wobei diese Speicherpflicht auf nur sieben Tage begrenzt wird und die gespeicherten Verkehrsdaten allein mittelbar für eine Bestandsdatenauskunft (§113 TKG) verwendet werden dürfen.[40]

---

gegenüber den Sicherheitsbehören als jede andere europäische Regelung, weil sie die Unternehmen in den Mitgliedstaaten zur Erzeugung und dauerhaften Speicherung riesiger Datensammlungen verpflichtet, die nach Maßgabe des nationalen Rechts einem weitgehenden behördlichen Zugriff für Zwecke der Sicherheit und der Strafverfolgung unterliegen.

[35] BGBl I 2008, S. 70.

[36] BVerfG Urt. Urt. v. 02.03.2010, BVerfGE 125, 260 ff.

[37] Prof. Dr. Nikolaus Frogo und Rain Dr. Tina Krügel in K&R 2010, S. 220

[38] Vgl. Prof. Dr. Markus Möstl, Zeitschrift für Rechtspolitik 2011, S. 226

[39] http://wiki.vorratsdatenspeicherung.de/images/DiskE_.pdf

[40] Prof. Dr. Markus Möstl, Zeitschrift für Rechtspolitik 2011, S. 226 rechte Spalte

Laut Presseerklärung der EU-Kommission vom 27.10.2011 [41] wurde Deutschland eine zweimonatige Frist zur Umsetzung der EU-Vorschriften zur Vorratsdatenspeicherung gesetzt.

Das Bundesjustizministerium hat am 16. August 2011 mitgeteilt, dass bereits ein Vorschlag zur Umsetzung der Richtlinie erstellt worden sei und man sich gerade in interministerieller Konsultation befände[42]. Ende Mai 2012 hat die EU-Kommission Klage gegen die Bundesrepublik Deutschland beim EuGH wegen Vertragsverletzung eingereicht.

2.2.4 Urteil des EuGH zur Unabhängigkeit des Datenschutzbeauftragten - Umsetzung

Die Europäische Kommission hatte am 05.07.2005 ein Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland eingeleitet. Mit der Klage verfolgte die Europäische Kommission die Absicht, die Bundesrepublik Deutschland zur Einführung eines im Sinne der EU- Datenschutzrichtlinie[43] unabhängigen Datenschutzbeauftragten zu bewegen.

Mit Urteil vom 09.03.2010 hat der EuGH entschieden, dass die Bundesrepublik Deutschland gegen ihre Verpflichtungen aus Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr verstoßen hat, indem sie die für die Überwachung der Verarbeitung personenbezogener Daten durch nicht-öffentliche Stellen und öffentlich-rechtliche Wettbewerbsunternehmen zuständigen Kontrollstellen in den Bundesländern staatlicher Aufsicht unterstellt und damit das Erfordernis, dass diese Stellen ihre Aufgaben „in völliger Unabhängigkeit" wahrnehmen, falsch umgesetzt hat.
In Bezug auf öffentliche Stellen bezeichne der Begriff „Unabhängigkeit" nach Auffassung des EuGH in der Regel eine Stellung, in der gewährleistet sei, dass die betreffende Stelle völlig frei von Weisungen und Druck handeln könne. Entgegen dem Standpunkt der Bundesrepublik Deutschland deute nichts darauf hin, dass das Unabhängigkeitserfordernis allein das Verhältnis zwischen den Kontrollstellen und den ihrer Kontrolle unterstellten Einrichtungen beträfe. Vielmehr werde der Begriff „Unabhängigkeit" noch durch das Adjektiv „völlig" verstärkt, was eine Entscheidungsgewalt impliziere, die jeglicher Einflussnahme von außerhalb der Kontrollstelle, sei es unmittelbar oder mittelbar, entzogen sei.

[41] http://www.presseportal.de/pm/35368/2137097
[42] Vgl. http://www.presseportal.de/pm/35368/2137097
[43] RL 95/46/EG, ABl. EG v. 23.11.1995, Nr. L 281, S. 31

Für den Bereich der Landeszentrale bestehen derartige Zweifel an der Unabhängigkeit des Beauftragten für den Datenschutz nicht; dieser ist nach Art. 20 Abs. 3 S. 6 BayMG in der Ausübung seines Amtes, auch bei der Aufsicht über die Landeszentrale selbst, unabhängig und nur dem Gesetz unterworfen.[44]

Da auch die gelebte Praxis bei der Landeszentrale diesen Vorgaben entspricht, dürften diese Verhältnisse auch den Vorstellungen der Europäischen Kommission im Hinblick auf Art. 28 Abs. 1 der EU- Datenschutzrichtlinie entsprechen, so dass für den Bereich der Landeszentrale wie auch ihrer Anbieter sicherlich richtlinienkonforme Bedingungen bestehen.

2.2.5 Richtlinie 2009/136/EG[45]

Am 25.11.2009 haben das Europäische Parlament und der Rat der Europäischen Union die Richtlinie 2009/136/EG und damit Änderungen der Datenschutzrichtlinie für elektronische Kommunikation[46] beschlossen und Art. 4 der E-Privacy-RL um eine Informationspflicht im Falle einer Verletzung des Schutzes personenbezogener Daten ergänzt. Nach dem neuen Art. 4 Abs. 3 S. 1 hat der Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste im Falle einer Verletzung des Schutzes personenbezogener Daten unverzüglich die zuständige nationale Behörde von der betreffenden Verletzung zu benachrichtigen. Nach Art. 4 Abs. 3 S. 2 n. F. hat er darüber hinaus auch die Teilnehmer bzw. betroffenen Personen unverzüglich von der Verletzung zu benachrichtigen, wenn anzunehmen ist, dass diese durch die Verletzung des Schutzes personenbezogener Daten in ihrer Privatsphäre beeinträchtigt werden.

Die hier vorgesehene Informationspflicht ist weitergehender als die bisher beispielsweise in § 42 a BDSG, § 15 a TMG und § 93 Abs. 3 TKG vorgesehenen. Die Informationspflicht greift danach nicht nur bei einer unrechtmäßigen Übermittlung von Daten, sondern darüber hinaus auch bei jeder Art von Sicherheitsverletzung, die auf unbeabsichtigte oder unrechtmäßige Weise zur Vernichtung, zum Verlust oder zur Veränderung der Daten führt. Das Qualifikationsmerkmal der „schwerwiegenden Beeinträchtigungen" wird in der Richtlinie nicht erwähnt. Die Dienstanbieter werden zudem verpflichtet, ein

[44] Vgl. dazu unten die Ausführungen zur Funktion des Beauftragten für den Datenschutz unter 3.
[45] 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.
[46] RL 2002/58/EG sog. E-Privacy-Richtlinie.

Verzeichnis der Verletzungen des Schutzes personenbezogener Daten zu führen. Die Richtlinie muss bis zum 25.05.2011 in nationales Recht umgesetzt werden. Nachdem die Frist zur Umsetzung bereits abgelaufen war, erfolgte die Umsetzung in der Novelle zum TKG vom 09.05.2012[47].

Zudem enthält die RL 2009/136/EG eine maßgebliche Änderung von Art. 5 Abs. 3 der E-Privacy-RL, die künftig eine Speicherung von Informationen oder den Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, im Wesentlichen nur gestattet, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen u.a. über die Zwecke der Verarbeitung seine Einwilligung gegeben hat.

In Deutschland gab es unterschiedliche Ansätze zur Umsetzung im TMG. Da sich jedoch Bundesrat und Bundestag nicht auf einen Vorschlag einigen konnten, steht die Umsetzung nach wie vor aus. Der Bundesbeauftrage für den Datenschutz und die Informationsfreiheit hält daher die E-Privacy-Richtlinie insoweit in Deutschland für unmittelbar anwendbar.

2.3 Bundesrecht

2.3.1. Bundesdatenschutzgesetz (BDSG)

2.3.1.1 Novelle I - III

Nachfolgend wird ein kurzer Überblick über die in drei Novellen im Bundesdatenschutzgesetz vorgenommenen Veränderungen gegeben, die bis 11.06.2010 sukzessive in Kraft getreten sind.[48]

- In der Neufassung des § 3 a BDSG wird nun für alle Erhebungen, Verarbeitungen und Nutzungen die Pflicht zur Datensparsamkeit und Anonymisierung festgelegt.

- Die Anforderungen an die Datenauftragsverwaltung gem. § 11 BDSG wurden verschärft. Neu ist, dass der Mindestgehalt des der Auftragsverwaltung zugrundeliegenden Vertrages nun gesetzlich detailliert vorgegeben wird.

[47] BGBl. I 2012, S. 958
[48] Zu den BDSG-Novellen wurde im 9. Tätigkeitsbericht, Punkt: 2.2.1, S.11-19, ausführlich berichtet.

Der Auftraggeber hat sich dabei erstmals vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen, was aus Gründen der Nachweisbarkeit zu dokumentieren ist.

- Einer der Kernpunkte der Neuregelungen war eine erhebliche Beschränkung der Verwendung personenbezogener Daten für die Zwecke des Adresshandels oder der Werbung gem. § 28 BDSG, wobei sich die Neuregelung durch ein reichhaltiges Regel- und Ausnahmegewirr auszeichnet. Neu geschaffen wurden die Vorschrift des § 28 a BDSG zur Datenübermittlung an Auskunfteien sowie des § 28 b BDSG zum Scoring.

- Nach den letzten Datenschutzskandalen ist zum Arbeitnehmerdatenschutz § 32 BDSG neu gefasst worden. § 32 Abs. 1 BDSG erfasst alle in einem abhängigen Beschäftigungsverhältnis stehenden Personen, vgl. § 3 Nr. 11 BDSG. Als Rechtsgrundlage für Daten, die in einem Arbeitsverhältnis benötigt werden, dient § 32 Abs. 1 BDSG. Die Generalklausel des § 28 Abs. 1 S.1 BDSG werden hierdurch im Hinblick auf Beschäftigungsverhältnisse konkretisiert und insoweit verdrängt. Auch das Ziel der Aufdeckung von Straftaten ist der Wortlaut des § 32 Abs. 1 S. 2 BDSG so eindeutig, dass diese Folge bei Anlegung rechtsstaatlicher Grundsätze zwingend erscheint. Personenbezogene Daten eines Beschäftigten dürfen gem. § 32 Abs. 1 S. 2 BSDG zur Aufdeckung von Straftaten nur dann erhoben, verarbeitet oder genutzt werden, wenn tatsächliche Anhaltspunkte (begründeter Verdacht) dafür vorliegen, dass der Beschäftigte eine Straftat begangen hat, die im Zusammenhang mit dem Beschäftigungsverhältnis steht.

- Die Novelle des BDSG brachte auch erhebliche Änderungen des bisherigen Sanktionsinstrumentariums bei Datenschutzverstößen mit sich. Der bisher gesetzlich vorgesehene Bußgeldrahmen bei Datenschutzverstößen wurde erhöht. Neu hinzugetreten ist auch eine Regelung, wonach diese Höchstbeträge im Einzelfall überschritten werden können; dies soll insbesondere die Abschöpfung des wirtschaftlichen Vorteils ermöglichen, den die verantwortliche Stelle aus den Datenschutzverstößen erlangt hat. Zudem ermächtigt § 38 Abs. 5 S. 1 BDSG die Aufsichtsbehörden ausdrücklich dazu, nicht nur die Maßnahmen zur Beseitigung festgestellter Verstöße anzuordnen, sondern sogar im Falle schwerwiegender Mängel die Datenerhebung und Verwendung oder den Einsatz einzelner Verarbeitungsverfahren insgesamt zu untersagen.

§ 42 a BDSG statuiert eine Informationspflicht von Unternehmen, wenn bei diesen eine sog. Datenschutzpanne eingetreten ist. Diese Datenschutzpanne muss allerdings die in § 42 a BDSG aufgeführten Daten betreffen. Eine Datenschutzpanne liegt vor, wenn diese Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind. Zudem müssen dem Betroffenen schwerwiegende Beeinträchtigungen materieller oder immaterieller Art drohen. Die verantwortliche Stelle muss in einem solchen Fall die zuständige Aufsichtsbehörde und den Betroffenen unverzüglich benachrichtigen. Da alle Betroffenen zu benachrichtigen sind, kann dies erhebliche Folgen haben.

Würde diese Benachrichtigung einen unverhältnismäßigen Aufwand erfordern, ist auch eine Information der Öffentlichkeit möglich. Da dies aber eine mindestens halbseitige Anzeige in zwei bundesweit erscheinenden Tageszeitungen bedeutet, dürfen die Auswirkungen dieser Alternative kaum als gering einzustufen sein, so dass angesichts der nunmehr vorgeschriebenen Folgen einer solchen Datenschutzpanne, entsprechende Vorkehrungen zur Vermeidung solcher Pannen höchst ratsam erscheinen.

2.3.1.2 Beschäftigtendatenschutz

Zum Arbeitnehmerdatenschutz ist im August 2010 ein Gesetzesentwurf[49] vorgelegt worden. Danach sollte der bisherige § 32 BDSG entfallen und der Beschäftigtendatenschutz umfassend in den Vorschriften §§ 32 a bis 32 l BDSG geregelt werden. Ziel war es, einerseits dem Arbeitnehmer Sicherheit hinsichtlich der Verwendung personenbezogener Daten zu geben, andererseits aber auch das Informationsinteresse des Arbeitgebers zu beachten.

Der Bundesrat nahm am 05. November 2010 zum Gesetzesentwurf Stellung[50], das Gesetz wurde jedoch bis ins Jahr 2012 immer noch nicht verabschiedet. Ob dies im Rahmen der laufenden Legislaturperiode noch erfolgen wird ist zumindest ungewiss.

2.3.1.3 Rote-Linie-Gesetz[51]

Das Bundesministerium des Inneren hat am 01. Dezember 2010 einen Gesetzesentwurf zum sogenannten „Rot-Linie-Gesetz" vorgestellt. Dieses soll das BDSG durch einen neuen § 38 b ergänzen, der die Rechte von Betroffenen bei Veröffentlichung von Daten in Telemedien stärken soll.

---

[49] Gesetzesentwurf Bundesregierung; BR-Drs. 535/10
[50] Stellungnahme BR-Drs. 535/10
[51] http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/rote_linie.pdf?__blob=publicationFile

Danach sollen solche Veröffentlichungen, die besonders schwerwiegend in das Persönlichkeitsrecht eingreifen, nur zulässig sein, sofern dies eine andere Rechtsvorschrift erlaubt, der Betroffene ausdrücklich eingewilligt hat oder ein überwiegendes schutzwürdiges Interesse an der Veröffentlichung besteht. Überdies enthält der Entwurf Vorschläge zur Regulierung von Internetdiensten, die für die Integrität der Persönlichkeitsrechte von besonderer Bedeutung sind.

Dies sind etwa Gesichtserkennungsdienste, mit denen Personen anhand biometrischer Merkmale im Internet identifiziert werden können, sowie Dienste zur Profilbildung anhand von Suchmaschinenanfragen und die Erhebung von Standortdaten von Mobiltelefonen und GPS-Smartphones. Vorgesehen ist, den Betroffenen künftig bei schweren Verletzungen des Persönlichkeitsrechts einen immateriellen Schadensersatzanspruch gegen Privatunternehmer an die Hand zu geben. Danach solle die Höhe des Schmerzensgeldes so bemessen sein, dass diese auch Präventionswirkung entfaltet.

Die eingeleitete Resort Abstimmung zu dem Gesetzesvorhaben wurde leider im Februar 2011 unterbrochen.

2.3.2 Telekommunikationsgesetz (TKG)

Im Berichtszeitraum war die bedeutendste Veränderung in datenschutzrechtlicher Hinsicht die Umsetzung der Vorgaben der bereits oben genannten Richtlinie 2006/24/EG[52] zur Vorratsdatenspeicherung. Zwar erfolgte die Umsetzung durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG[53], das am 01.01.2008 in Kraft trat. Jedoch wurde durch Bundesverfassungsgericht mit Urteil vom 02. März 2010[54] entschieden, dass die für die Vorratsdatenspeicherung maßgelblichen Vorschriften der §§ 113 a und 113 b TKG (sowie der StPO) mit Art. 10 Abs. 1 GG nicht vereinbar sind. Eine Neuregelung ist bisher nicht erfolgt.[55]

[52] Vgl. oben 2.2.3.
[53] BGBl. I 2007, S. 3198.
[54] BVerfG Urt. v. 02.03.2010, BVerfGE 125, 260 ff,.
[55] Siehe hierzu näheres unter Punkt 2.2.3

Weiterhin waren die EU-Richtlinien 2009/140/EG[56] und 2009/136/EG[57] umzusetzen, was mit Gesetz vom 03.05.2012[58] erfolgte, das die folgenden in datenschutzrechtlicher Hinsicht bedeutsamen Vorschriften neu fasste:

- In § 91 Abs. 1 TKG wurde der Anwendungsbereich auf Telekommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen, erweitert, womit insbesondere RFID-Funkfrequenzerkennungsgeräte vom Datenschutz im TKG erfasst wurden.[59] Die Radio Frequency Identification Devices (RFID) können sehr unterschiedliche Verwendungen finden von der Fahrzeugsicherung, Warenflusskontrolle, Transport und Logistik bis zu Gebrauchsgütern des täglichen Bedarfs und dadurch für den Bürger durchaus auch erhebliche Bedeutung erlangen.

- § 92 TKG wurde gestrichen. Infolgedessen regeln die Vorschriften der §§ 4b und 4c BDSG die Übermittlung personenbezogener Daten ins Ausland abschließend.[60]

- Um die Transparenz der Datenverarbeitung zu verbessern, wurden die Informationspflichten des Dienstanbieters in § 93 Abs. 3 TKG und durch den neuen § 109 a TKG erweitert.

- Im Hinblick auf § 98 TKG wurde die Definition von Standortdaten in § 3 Nr. 19 TKG klarstellend dahin ergänzt, dass nun auch die direkt von einem Endgerät erhobenen Daten zur Lokalisation Standortdaten sind.[61] § 98 Abs. 1 Satz 1 TKG regelt, dass Standortdaten nur anonym erhoben werden dürfen, sofern der Teilnehmer keine Einwilligung erteilt hat.

- In § 108 TKG werden neue Sicherheitsanforderungen und Benachrichtigungspflichten für den Notruf vorgegeben.

2.3.3 Telemediengesetz (TMG)

Die zuletzt in datenschutzrechtlicher Hinsicht maßgeblichen Veränderungen des TMG erfolgten im Jahr 2009 [62]. Dabei wurde der ursprüngliche § 12 Abs. 3 TMG und das darin niedergelegte Koppelungsverbot aufgehoben[63].

[56] RL 2009/140/EG, ABl. L 337 v. 18.12.2009, 37.
[57] RL 2009/136/EG, ABl. L 337 v. 18.12.2009, 11.
[58] BGBl. 2012 I 2012, S. 958.
[59] Roßnagel/Johannes/Kartal, Die TK-Novelle, K&R 2012, S. 250.
[60] Roßnagel/Johannes/Kartal, Die TK-Novelle, K&R 2012, S. 250.
[61] Roßnagel/Johannes/Kartal, Die TK-Novelle, K&R 2012, S. 250.
[62] Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 14.08.2009, BGBL. I. 2009, S. 2814.
[63] Näheres hierzu siehe 9. Tätigkeitsbericht S. 30/31.

Im Übrigen wird im neuen § 15a TMG für Datenpannen auf den oben dargestellten[64] mit der BDSG-Novell II eingefügten § 42a BDSG und die darin vorgesehenen z.T. schwerwiegenden Folgen verwiesen.

Daneben hätte auch die Richtlinie 2009/136/EG [65] und damit die Änderung des Art. 5 Abs. 3 der E-Privacy-Richtlinie (2002/58/EG), die den Einsatz von Cookies beschränkt und den Gebrauch von Cookies von der vorherigen Einwilligung des Nutzers abhängig macht, bis zum Mai 2011 umgesetzt werden müssen.[66]

Hierfür, aber auch zur Verbesserung des Datenschutzes bei Telemedienangeboten mit nutzergenerierten Inhalten hat der Bundesrat am 17.06.2011 einen Gesetzesentwurf beschlossen[67], der umfangreiche Änderungen im TMG, insbesondere zusätzliche Pflichten für Anbieter von Telemedien mit nutzergenerierten Inhalten vorsieht.

So sollen z.B. die Informationspflichten der Diensteanbieter gegenüber den Nutzern verstärkt werden. Es sollen Datenschutzhinweise 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.

Die Bundesregierung ist zwar der Ansicht, dass der Gesetzesentwurf wichtige Themen aufgreife, die den Datenschutz bei Internetangeboten mit nutzergenerierten Inhalten, insbesondere Sozialen Netzwerken betreffen, und auch sie strebe mit Blick auf einen effektiven Kinder- und Jugendmedienschutz ein besonders hohes Datenschutzniveau an. Allerdings werfe der Vorstoß des Bundesrates derzeit Fragen auf, die zunächst der Klärung bedürften.

---

[64] Vgl. oben 2.3.1.1.
[65] Siehe Fn. 44
[66] Siehe 2.2.5
[67] BR Drs. 156/11.

Diese konnten bisher offenbar noch nicht geklärt werden, zumal Geltungsbereich und künftige Bedeutung der umzusetzenden E-Privacy-Richtlinie aufgrund der Planungen zur EU-Datenschutz-Grundverordnung[68] auch schon nach Europarecht keineswegs mehr eindeutig erscheinen.

2.3.4 Allgemeines Gleichbehandlungsgesetz (AGG)

Das allgemeine Gleichbehandlungsgesetz wurde zwar im Berichtszeitraum verändert. Diese Änderungen haben jedoch auf den Bereich des Datenschutzes keinerlei Auswirkungen, so dass insoweit auf den vorangegangenen Tätigkeitsbericht verwiesen werden kann.

2.3.5 Informationsfreiheitsgesetz des Bundes (IFG)

Das Bundesverwaltungsgericht hat am 03.11.2011[69] entschieden, dass das Informationsfreiheitsgesetz grundsätzlich für die gesamte Tätigkeit der Bundesministerien gilt.

Im o.g. Verfahren begehrte der Kläger Einsicht in bestimmte Unterlagen des Bundesjustizministeriums. Diese waren interne Vorlagen an die Ministerin im Zusammenhang mit der Untersuchung einer etwaigen Reformbedürftigkeit des Kindschaftsrechts und die Stellungnahmen des Bundesjustizministeriums vor dem Petitionsausschuss des Bundestags zur Frage der Rehabilitierung der Opfer der sog. Bodenreform in der Sowjetischen Besatzungszone. Das Bundesverwaltungsgericht stellt klar, dass das Bundesjustizministerium eine Behörde im Sinne des § 1 IFG ist.

Eine Unterscheidung zwischen Verwaltungshandeln und Regierungshandeln nehme das IFG nicht vor. Eine solche Differenzierung stünde dem Zweck des Gesetzes entgegen. Daran ändere auch nichts, dass die Stellungnahme vor dem Petitionsausschuss im Rahmen einer Verfassungspflicht erfolgte. Gesetzliche Versagungsgründe i.S.d. §§ 3 ff. IFG lägen nicht vor, auch auf Vertrauensschutz könne die Versagung nicht gestützt werden.

2.3.6 Gesetz über das Verfahren des elektronischen Entgeltnachweises (sog. ELENA-Verfahrensgesetz) vom 28.03.2009

Am 28.03.2009 wurde das Gesetz über das Verfahren des elektronischen Entgeltnachweises (sog. ELENA-Verfahrensgesetz)[70] beschlossen. Das Gesetz trat am 01.01.2010 in Kraft.

---

[68] vgl. Art. 89 EU-Datenschutz-Grundverordnung der das künftige Zusammenspiel mit der E-Privacy-Richtlinie (2002/58/EG) wohl nur scheinbar klar regelt.
[69] BVerwG Urt. v. 03.11.2011 7 C 4.11
[70] BGBl. I 2009, S. 634 f.

Das ELENA-Verfahren verfolgt das Ziel, die Arbeitgeber künftig von der aufwändigen Erstellung einer Vielzahl von Bescheinigungen zu entlasten und gleichzeitig das Verfahren für die Antragsteller zu vereinfachen. Zu diesem Zweck wurden die Arbeitgeber ab dem 1. Januar 2010 gesetzlich verpflichtet, monatlich eine entsprechende ELENA-Meldung an die zentrale Speicherstelle zu versenden, damit die bisher von den Arbeitgebern auf Papier erstellten Gehaltsbescheinigungen in Verfahren vor Sozialbehörden elektronisch aus diesen Speichern zur Verfügung stehen.

In der zentralen ELENA-Datenbank wurden ab dem 01.01.2010 die entsprechenden Daten der Betroffenen gespeichert, sollten aber erst ab dem 1. Januar 2012 von den ausdrücklich dazu befugten Stellen einzelfallbezogen abgerufen werden können. Mit diesem Verfahren sollte wiederum aufgrund eines Gesetzes eine große zentrale Datensammlung mit personenbezogenen Daten geschaffen werden, die schon alleine für sich betrachtet, aber vor allem im Zusammenspiel mit anderen Daten aufschlussreiche Rückschlüsse weit jenseits der Frage des individuellen Gehalts des Betroffenen erlaubt hätte, ohne dass der einzelne Bürger dazu einen Anlass gegeben hätte.

Hintergrund hierfür ist, dass nicht nur die tatsächlichen Gehaltszahlungen, sondern auch Schwankungen des regelmäßigen Gehaltes und die hierfür maßgeblichen Gründe angegeben, zentral gesammelt und in einer Datenbank gespeichert werden sollten. Als besonders problematisch wurden Angaben über krankheits- oder gar arbeitskampfbedingte Ausfalltage angesehen.

Datenschützer hatten während des gesamten Entstehungsprozesses erhebliche Bedenken angemeldet. Zentrale Kritikpunkte waren einerseits, dass die Daten zentral, anlasslos und sogar auch zu Personen erhoben werden sollten, bei denen es zumindest sehr unwahrscheinlich ist, dass die Daten tatsächlich jemals gebraucht werden könnten. Andererseits wurde aber auch die Detailtiefe der Datenabfrage problematisiert.

Am 31.03.2010 wurde Verfassungsbeschwerde gegen den elektronischen Einkommensnachweis ELENA in Karlsruhe eingereicht. Daneben fand eine politische Diskussion vor allem auch zu den besonders vehement kritisierten Angaben zu Fehlzeiten und arbeitsrechtlichen Vorgängen statt. Die Arbeitgeber hatten der gleichwohl existierenden Meldepflichten nachzukommen.

Mitte 2011 kam es zur Kehrtwende. In einer gemeinsamen Presseerklärung des Bundesministeriums für Wirtschaft und Technologie und des Bundesministeriums für Arbeit und Soziales vom 18. Juli 2011[71] wurde mitgeteilt, dass man sich nach eingehender Überprüfung des ELENA-Verfahrens geeinigt habe, dies schnellstmöglich einzustellen. Grund hierfür sei die fehlende Verbreitung der qualifizierten elektronischen Signatur. Die Bundesregierung werde dafür Sorge tragen, dass alle bisher gespeicherten Daten unverzüglich gelöscht und die Arbeitgeber von der Meldepflicht entbunden würden.

Mit dem Gesetz zur Änderung des Beherbergungsstatistikgesetzes und des Handelsstatistikgesetzes sowie zur Aufhebung von Vorschriften zum Verfahren des elektronischen Entgeltnachweises vom 23.11.2011, das zum 01.01.2012 in Kraft trat[72], wurde das ELENA-Verfahren eingestellt.

In seiner Presseerklärung vom 08.11.2011[73] erklärt der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Peter Schaar, er habe den Datenbankhauptschlüssel des Verfahrens zum Elektronischen Entgeltnachweis (ELENA) gelöscht.

„Nur mit diesem digitalen Schlüssel war der Zugriff auf die verschlüsselt gespeicherten Entgeltdaten von mehr als 35 Millionen Arbeitnehmern möglich".[74]

2.3.7 Novellierung des „Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (sog. BKA-Gesetz)

Am 1. Januar 2009 ist die Novellierung des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten[75] in Kraft getreten.

Die Änderungen im BKA-Gesetz waren darauf ausgerichtet, den Beamten des Bundeskriminalamtes umfangreiche neue Befugnisse einzuräumen, um die Bekämpfung des internationalen Terrorismus zu verbessern.[76] Neben der Online-Durchsuchung regeln die neuen Vorschriften des BKA-Gesetzes u.a.

[71] http://www.bmwi.de/DE/Presse/pressemitteilungen,did=424742.html
[72] BGBl. 2011, S. 2299
[73] http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2011/40_ELENA.html
[74] http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2011/40_ELENA.html
[75] Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt vom 25.12.2008, BGBl. I 2008, S. 3083.
[76] Vgl. § 20a - § 20x BKAG.

die Rasterfahndung, den Einsatz verdeckter Ermittler, akustische und optische Überwachung von Wohnungen und die Telekommunikationsüberwachung.

Zahlreiche Institutionen bis hin zum Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, vor allem aber auch Journalisten- und Medienverbände haben zu dem Gesetzentwurf zumeist kritisch Stellung genommen. Sie kritisierten die aus ihrer Sicht unverhältnismäßigen Befugnisse der Ermittlungsbehörden und warnten vor einer Aushöhlung des Zeugnisverweigerungsrechts für Journalisten und andere Berufsgeheimnisträger. Problematisch sei hierbei, dass neben der Telekommunikationsüberwachung und der Durchsuchung des Computers auch die Herausgabe der Inhalte dieser Kommunikation erzwungen werden könne, weil das Bundeskriminalamt Telefongespräche abhören, E-Mail-Verkehr aufzeichnen und auf Kommunikationsdaten der letzten Monate zugreifen könne, wenn die nach diesem Gesetz vorgesehene einfache Verhältnismäßigkeitsprüfung ein positives Ergebnis erbracht habe. Bereits durch die Möglichkeit einer Vorratsdatenspeicherung würden potentielle Informanten abgeschreckt, sich mit vertraulichen Informationen an Journalisten zu wenden; dieser Effekt würde durch das BKA-Gesetz nochmals verschärft.

Am 27. Januar 2009 wurde eine Verfassungsbeschwerde gegen die Neuregelungen des BKA-Gesetzes eingereicht. Gerügt wurde hierbei die Verletzung des Rechts auf informationelle Selbstbestimmung, des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und die Verletzung des Art. 10 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Über diese ist bisher noch nicht entschieden worden.

Das BKA-Gesetz hat durch das Gesetz vom 21. Juli 2012 über die Vereinfachung des Austausches von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union Veränderungen erfahren, die z.T. auch datenschutzrechtliche Relevanz entfalten.

2.3.8 Entwurf eines Bundesmeldegesetzes

Das Bundesministeriums des Inneren teilt auf seiner Internetseite mit, dass der Bund die ihm zustehende ausschließliche Gesetzgebungskompetenz für das Meldewesen gemäß Art. 73 Abs. 1 Nr. 3 GG in dieser Legislaturperiode durch ein Bundesmeldegesetz wahrnehme.[77] Die Bundesregierung hat zum 31.08.2011 einen Gesetzentwurf beschlossen, danach soll das Melderecht in

[77] http://www.bmi.bund.de/SharedDocs/Standardartikel/DE/Themen/OeffentDienstVerwaltung/Meldewesen/ausblick.html?nn=2237178

Deutschland harmonisiert und fortentwickelt werden. Es soll erstmals bundesweit einheitliche und unmittelbar geltende melderechtliche Vorschriften für alle Bürger und Bürgerinnen geben. Am 16.11.2011 wurde der Entwurf eines „Gesetzes zur Fortentwicklung des Meldewesens (MeldFortG)“[78] vorgelegt. Der Entwurf des Gesetzes sieht eine Stärkung des Rechts auf informationelle Selbstbestimmung der Bürger und Bürgerinnen vor und baue für die Wirtschaft Bürokratiekosten in Höhe von rund 117 Mio. Euro pro Jahr ab. Weiterhin werde hierdurch die Bekämpfung von Scheinanmeldungen intensiviert und zudem der Online-Zugang öffentlicher Stellen zu Meldedatenbeständen verbessert. Laut Pressemitteilung des Bundesministeriums des Inneren[79] seien folgende wesentliche Neuregelungen vorgesehen:

- Soweit Melderegisterauskünfte zur gewerblichen Nutzung erfragt werden, ist zukünftig der Zweck der Anfrage anzugeben und die Melderegisterauskunft ausschließlich zu diesem Zweck zu verwenden; Meldeauskünfte für Zwecke der Werbung und des Adresshandels sind nur noch mit Einwilligung der betroffenen Person möglich.

- Sicherheitsbehörden und weitere, durch andere Rechtsvorschriften zu bestimmende Behörden sollen rund um die Uhr länderübergreifend einen Online-Zugriff für die Meldedaten erhalten.

- Die Hotelmeldepflicht sowie das Verfahren bei Aufenthalten in Krankenhäusern, Heimen u. ä. Einrichtungen werden vereinfacht.

- Die Mitwirkungspflicht des Vermieters bei der Anmeldung von Mietern soll wieder neu eingeführt werden, um Scheinanmeldungen und damit häufig verbundenen Formen der Kriminalität wirksamer zu begegnen.

Der Bundestag hat sodann am 26.04.2012 über den Gesetzesentwurf in erster Lesung debattiert.[80] In zweiter und dritter Lesung wurde der Gesetzesentwurf mit einigen wesentlichen Änderungen am 28.06.2012 beschlossen. Danach entstand eine öffentliche Diskussion über die Weitergabe der Meldedaten an Dritte. Am 21.09.2012 hat der Bundesrat den Vermittlungsausschuss angerufen.

[78] BT-Drs. 17/7746
[79] Vgl. Fn. 77
[80] Erste Beratung: BT-PlPr 17/175, S. 2078 1C – 2078 6C

2.4 Bayerisches Landesrecht

2.4.1 Änderung des BayDSG

Aufgrund des Urteils des EuGH zur Unabhängigkeit des Datenschutzbeauftragten[81] wurde in Bayern erstmals mit der Fünften Verordnung zur Änderung der Datenschutzverordnung vom 20. April 2011 auf das EuGH-Urteil reagiert.[82] In § 1 Nr. 2 Satz 2 DSchV wurde der Wortlaut wie folgt gefasst: „Das Landesamt für Datenschutzaufsicht nimmt seine Aufgaben in völliger Unabhängigkeit wahr."

Danach wurde die Aufsichtstätigkeit für den nicht-öffentlichen Bereich von der bis dahin zuständigen Regierung von Mittelfranken auf eine den Vorgaben des o.g. EuGH-Urteils entsprechende neue Stelle verlagert. Seit der Gesetzesänderung des BayDSG und anderer Rechtsvorschriften vom 20. Juli 2011[83] wird in Art. 34 BayDSG die Zuständigkeit des nunmehr eigenständigen Landesamtes für Datenschutz in Ansbach geregelt.

In Art. 35 BayDSG wurde die Unabhängigkeit der Aufsichtsbehörde und seines Präsidenten manifestiert. Mit Inkrafttreten der geänderten Vorschriften zum 01. August 2011 wurde Herr Thomas Kranig zum Präsidenten des Landesamtes für Datenschutzaufsicht ernannt.

2.4.2 Rundfunkstaatsvertrag

2.4.2.1 Rundfunkgebührenstaatsvertrag

Der 15. Rundfunkänderungsstaatsvertrag wurde von den Regierungschefs vom 15. – 21.12.2010 unterzeichnet und fristgemäß zum 31.12.2011 von den Länderparlamenten ratifiziert. Er tratt am 1. Januar 2013 in Kraft, wobei einige Übergangsvorschriften nach § 14 Abs. 1, 2 und 6 Rundfunkbeitragsstaatsvertrag (RBeitrStV) bereits am 1. Januar 2012 in Kraft getreten waren.

Der Rundfunkbeitragsstaatsvertrag sieht vor, dass pro Haushalt (Wohnung) ein Beitrag in Höhe von € 17,98 entrichtet werden soll. Damit sind alle Nutzungsmöglichkeiten der dort lebenden Personen abgegolten. Das betrifft etwa auch im Haushalt lebende Kinder mit eigenem Einkommen. Gleiches gilt im nicht privaten Bereich, d. h. der Beitrag wird pro Betriebsstätte gestaffelt nach Anzahl der Mitarbeiter erhoben. Dabei gibt es für Kleinbetriebe mit bis zu vier Mitarbeitern einen ermäßigten Beitragssatz von einem Drittel.

[81] S.o. 2.2.4
[82] BayGVbl. Nr. 8/2011, S. 186
[83] BayGVbl. Nr. 14/2011, S. 307-308

Das Gesetzgebungsverfahren zum neuen Rundfunkbeitragsstaatsvertrag wurde von den Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio begleitet. Nach deren Stellungnahme vom 15.09.2010 trage der Rundfunkbeitragsstaatsvertrag den Belangen des Datenschutzes besser Rechnung, da Nachforschungen vor Ort minimiert werden könnten. Ebenfalls würde sich dadurch der Einsatz von Rundfunkgebührenbeauftragten deutlich reduzieren lassen. Künftig würden weniger Daten erhoben werden, da die Angaben zu Art und Anzahl der bereitgehaltenen Geräte entfallen könne und da die Beitragspflicht nicht mehr von den persönlichen Lebensverhältnissen von Menschen, die gemeinsam in einer Wohnung leben, abhängig gemacht würde.

Grundsätzlich seien die Daten beim Betroffenen jeweils direkt zu erheben. Auskunftsrechte der Landesrundfunkanstalt gegenüber öffentlich und nicht öffentlichen Stellen gemäß § 11 Abs. 4 RBeitrStV ohne Kenntnis der Betroffen dürften grundsätzlich nur nachrangig geltend gemacht werden.

Die Stellungnahme des AK DSB sieht auch in dem einmaligen Meldedatenabgleich, der es möglich mache, die anlässlich der Systemumstellung bisher nicht erfassten Beitragsschuldner zu ermitteln, keine datenschutzrechtlichen Verstöße. Hiermit würden Erhebungen vor Ort bei einer Vielzahl von Beitragsschuldnern entbehrlich. Sofern also für eine Wohnung ein Beitragsschuldner festgestellt werde, müssten die Daten der übrigen dort wohnenden Personen unverzüglich gelöscht werden, sobald das Beitragskonto ausgeglichen sei. Insgesamt würden somit nur die Daten Zahlungspflichtiger langfristig gespeichert werden.

In datenschutzrechtlicher Hinsicht wurde heftig diskutiert, ob die intensive Nutzung von Melderegisterdaten zu Rundfunkgebührenzwecken unverhältnismäßig sei. Die Einschätzungen hinsichtlich der Gewährleistung des Datenschutzes waren jedoch seitens der Landesbeauftragten für den Datenschutz und den Vertretern der Rundfunkanstalten sehr unterschiedlich. Während die Landesbeauftragten eklatante Normdefizite beklagten, waren die Vertreter der Rundfunkanstalten der Ansicht, es seien in die Normen des Rundfunkbeitragsstaatsvertrags Befugnisse hineingelesen worden, von denen die Rundfunkanstalten gar keinen Gebrauch machen wollten. Es kam daraufhin zu einem Gedankenaustausch, den ARD, ZDF und Deutschlandradio in einem Eckpunktepapier zusammenfassten.[84] Ziel des Papiers ist es, sich in unterschiedlichen Standpunkten anzunähern und Lösungen anzustreben, die einen effizienten Gebühren/Beitragseinzug gewährleisten, gleichzeitig aber auch datenschutzrechtlichen Erfordernissen Rechnung zu tragen.

[84] Eckpunkte von ARD, ZDF und Deutschlandradio für eine Konkretisierung der datenschutzrechtlichen Regelungen im Vollzug des 15. RÄndStV entwickelt und im November 2011 veröffentlicht.

2.4.2.2 BGH-Entscheidung zu Gunsten des Medienprivilegs

Mit Urteil des BGH vom 01.02.2011 [85] hat sich der Bundesgerichtshof mit dem Anwendungsbereich und den Grenzen des sogenannten Medienprivilegs befasst. In seinem Urteil vom 1. Februar 2011 gab der BGH im Fall des Mörders des Schauspielers Walter Sedlmayer der Medien- und Meinungsfreiheit den Vorrang gegenüber dem Datenschutz. Der verurteilte Mörder des bekannten Schauspielers Walter Sedlmayer, der im Januar 2008 auf Bewährung entlassen worden war, hatte gegen einen Artikel der Beklagten, den diese auf ihrem Nachrichtenportal im Internet am 12. April 2005 veröffentlicht hatte, geklagt. In diesem Artikel wurde der Kläger unter vollem Namen genannt. Dieses wollte er wegen seines Interesses an einer Wiedereingliederung in die Gesellschaft verhindern.

Der BGH stellte fest, dass das Informationsinteresse der Öffentlichkeit und das Recht auf freie Meinungsäußerung im vorliegenden Fall das Interesse des Straftäters überwiegen würden. Die Abwägung der Interessen habe ergeben, dass zwar das Bereithalten des Artikels ein Eingriff in das allgemeine Persönlichkeitsrecht des Klägers darstellen würde, dieser aber nicht rechtswidrig sei.

Das Wiedereingliederungsinteresse sei bei der Abwägung zwar von Bedeutung, jedoch sei die Beeinträchtigung durch die Namensnennung nicht erheblich. Die sachbezogene und objektive Darstellung wahrheitsgemäßer Aussagen über ein aufsehenerregendes Kapitalverbrechen an einem bekannten Schauspieler sei nicht geeignet, den Kläger ewig an den Pranger zu stellen oder neu zu stigmatisieren. Über dies sei der Bericht in einem Archivbereich des Portals abgelegt worden und ausdrücklich als Altmeldung gekennzeichnet worden. Der BGH stellte klar, dass ein generelles Löschgebot aller früheren, den Täter identifizierenden Darstellungen der Tat den freien Informations- und Kommunikationsprozess einschnüren und die Meinungs- und Medienfreiheit unzulässig einschränken würde. Zudem bestünde ein anerkennenswertes Interesse der Öffentlichkeit nicht nur an der Information über das aktuelle Zeitgeschehen, sondern auch an der Möglichkeit vergangene zeitgeschichtliche Ereignisse zu recherchieren. Dementsprechend würden die Medien ihre Aufgabe, in Ausübung der Meinungsfreiheit die Öffentlichkeit zu informieren und an der demokratischen Willensbildung mitzuwirken, auch dadurch wahrnehmen, dass sie nicht mehr aktuelle Veröffentlichungen für interessierte Mediennutzer verfügbar halten.

[85] VI. BGH Urt. v. 01.02.2011 ZR 345/09

Insgesamt stellte der BGH fest, dass vorliegend das Medienprivileg des Rundfunkstaatsvertrags aus § 57 Abs. 1 Satz 1 RStV einschlägig sei, das den Anwendungsbereich der allgemeinen Bestimmungen des Bundesdatenschutzgesetzes eingeschränke, denn der Beitrag sei, wie es der Rundfunkstaatsvertrag verlange, ausschließlich zu eigenen journalistisch redaktionellen Zwecken bereit gehalten worden. Es komme nicht auf die Frage an, wer sich auf das Medienprivileg berufen könne, nicht auf die Form der Veröffentlichung, sondern ausschließlich auf die Tätigkeit selbst, die eine publizistische sein müsse. Auch Internetportale würden sich nach Aussage des BGH somit auf diesen Schutz berufen können. Der zentrale Satz des Urteils lautet: „Ohne die Erhebung, Verarbeitung und Nutzung personenbezogener Daten auch ohne Einwilligung des jeweils Betroffenen wäre journalistische Arbeit nicht möglich – die Presse könnte ihre in Artikel 5 Abs. 1 Satz 2 GG, Art. 10 Abs. 1 Satz 2 EMRK, Art. 11 Abs. 1 Satz 1 der Carta der Grundrechte der Europäischen Union zuerkannten und garantierten Aufgaben nicht wahrnehmen."

2.4.3 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 Rechung trägt und andererseits ausdrücklich das Medienprivileg aufnimmt, hat sich 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 eine genaue Kenntnis der rechtlichen, wirtschaftlichen und programmlichen Verhältnisse besteht. Daneben stellt die gewählte Gestaltung aber auch sicher, dass bei der Rechtsanwendung die spezifischen Bedingungen des Rundfunks wie auch die bestehenden verfassungsrechtlichen Besonderheiten Berücksichtigung finden.

Ferner ist eine Abgrenzung zwischen Erhebung, Verarbeitung und Nutzung personenbezogener Daten, die dem Medienprivileg unterfallen, und Verwaltungsangelegenheiten der Landeszentrale bzw. der Anbieter entbehrlich, da die Aufsicht 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[86], und zwar auch, soweit es sich um Verwaltungsangelegenheiten handelt.[87] Mit dieser umfassenden Zuständigkeit für alle Aufgaben bei der Landeszentrale und den Anbietern trägt das BayMG den verfassungsrechtlichen Anforderungen an einen rundfunkrechtlichen Datenschutz Rechung.[88]

Weitere Aufgaben des Datenschutzbeauftragten sind die Beratung der Geschäftsführung bei datenschutzrechtlichen Fragen, die Mitarbeiterschulung in der Landeszentrale und die Beratung von Anbietern bei datenschutzrechtlichen Problemen.

Der Datenschutzbeauftragte hat bei der Durchführung seiner Aufgaben Auskunfts-, Kontroll-, Zugriffs-, Einsichts- und Beanstandungsrechte.[89]

---

[86] 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.

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

[88] 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.“

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

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 und zweckmäßig. Da der Datenschutzbeauftragte 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 Datenschutzbeauftragten bei der Landeszentrale 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 der EU-Datenschutzrichtlinie[90], die in Art. 28 Abs. 1 den Mitgliedsstaaten auferlegt, datenschutzrechtliche Kontrollstellen zu schaffen, die die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahrnehmen. Die Erfüllung dieser Vorgabe war in der Vergangenheit für die Aufsicht über den nicht-staatlichen Bereich in der Bundesrepublik nicht unumstritten. Die Europäische Kommission hatte am 5. Juli 2005 ein Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland eingeleitet, in dem die Kommission monierte, dass die Datenschutzaufsicht über die Privatwirtschaft, wie sie zum damaligen Zeitpunkt organisiert war, nicht in allen Fällen über die geforderte „völlige Unabhängigkeit" verfüge. Das Verfahren wurde in der Zwischenzeit vom Europäischen Gerichtshof durch Urteil[91] vom 09.03.2010 im Sinne der Europäische Kommission entschieden.[92] Die Gestaltung nach dem BayMG wurde dabei nicht angesprochen.

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.[93]

[90] RL 95/46/EG, ABl. EG v.23.11.1995, Nr. L 281/31.
[91] EuGH Urt. v. 09.03.2010, C- 518/07.
[92] Vgl. hierzu oben 2.2.4
[93] Vgl. Art. 20 Abs. 3 Satz 1 BayMG.

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 den durch den Präsidenten geleiteten Verwaltungsaufbau. Es besteht lediglich eine interne Dienstaufsicht, die durch den Verwaltungsrat wahrgenommen wird.

Die von der EU-Datenschutzrichtlinie geforderte und vom Europäischen Gerichtshof bestätigte völlige Unabhängigkeit des Beauftragten für den Datenschutz bei der Landeszentrale ist daher zweifelsfrei gegeben. Die Landeszentrale war daher von dem o.g. Verfahren nicht betroffen. Gelegentlich erhobene anderslautende Auffassungen sind inhaltlich unzutreffend.

4. Datenschutz in der Landeszentrale

4.1 Allgemeines

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.

Vom Bereich Presse wurde die datenschutzrechtliche Freigabe der BLM Homepage und der damit verbundenen Verfahren beantragt. Diese wurden umfassend geprüft, in Zusammenarbeit mit den Bereichen Presse und EDV gemeinsam erläutert und auf den aktuellen gesetzlichen Standard angepasst.

Im Berichtszeitraum ist kein weiteres Verfahren vorgelegt worden. Derzeit wird eine Bestandserhebung aller auch der nicht freigabepflichtigen automatisierten Verfahren, die personenbezogene Daten verarbeiten, durchgeführt.

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 Verzeichnis 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

Obwohl nach Art. 27 BayDSG die vormals bestehende Pflicht zur Führung eines Anlageverzeichnisses weggefallen ist, ist mit der EDV-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 werden und daher im Anlagespiegel gem. § 268 Abs. 2 HGB geführt werden müssen. 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 als gelöst angesehen werden.

Nennenswerte Auffälligkeiten konnten im Berichtszeitraum nicht festgestellt werden.

4.3 Mitarbeiter / Anfragen aus den Bereichen

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.

Im Berichtszeitraum wurde aus allen Bereichen Anfragen an den Datenschutzbeauftragten gerichtet. Soweit die angesprochenen Themen von allgemeinem Interesse sind, werden diese im Folgenden dargestellt.

4.3.1.1 Auftragsdatenverarbeitung

Fraglich war, ob bestimmte Dienstleistungen für die Landeszentrale in den Bereich der Funktionsübertragung oder der Auftragsdatenverarbeitung fallen und welche organisatorischen Schlussfolgerungen daraus zu ziehen sind.

Da sich in der BLM ebenso wie bei anderen Unternehmen Konstellationen ergeben, bei denen externe Unternehmen im Auftrag der Landeszentrale tätig werden und dabei personenbezogene Daten verarbeiten, wurden die gesetzliche Anforderungen an die Auftragsdatenverarbeitung aufgrund einer aktuellen Anfrage noch einmal unter den verschärften Auflagen des § 11 BDSG beleuchtet.

Durch die BDSG-Novelle vom 14. August 2009 wurden die Anforderungen an die Auftragsdatenverarbeitung nach § 11 Abs. 2 Satz 2 BDSG erweitert und in einem 10 Punktekatalog die Mindestanforderungen des Inhalts des zu erteilenden Auftrags festgehalten:

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die zu treffenden technischen und organisatorischen Maßnahmen (vgl. § 9 BDSG),
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen (vgl. § 11 Abs. 4 BDSG),
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,

8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,

9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,

10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Während diese Vorgaben vom Bundesgesetzgeber 2009 in das BDSG eingefügt wurden, blieb die Parallelvorschrift des Art.6 BayDSG unverändert. Eine Anpassung der Vorschriften über die Auftragsdatenverarbeitung im BayDSG an die expliziten Vorschriften des BDSG ist zwar langfristig angedacht, aber in der laufenden Legislaturperiode nicht mehr zu erwarten.

Art. 6 BayDSG ist daher so auszulegen, dass auch im Anwendungsbereich dieser Vorschrift die Wertungen des § 11 BDSG zu berücksichtigen sind. Der „Katalog" des § 11 Abs. 2 Satz 2 BDSG ist ggf. im Sinne einer Checkliste auch für Aufträge nach Art. 6 BayDSG zur Überprüfung heranzuziehen.

4.3.2 Internetauftritte und Facebook Like-Button

Es waren Fragen hinsichtlich des Impressums und der Datenschutzerklärung u. a. zur BLM-Homepage zu beantworten. Diese Fragen konnten im Berichtszeitraum stets in Zusammenarbeit mit der Abteilung EDV und dem Pressebereich umfassend gelöst werden.

Im Rahmen der Überprüfung der BLM-Homepage sowie bei der Bearbeitung von Beschwerden zu Internetradioanbietern waren zudem Fragen zur Zulässigkeit der Einbindung des Facebook Like-Buttons zu klären.

Im August 2011[94] hatte das unabhängige Landeszentrum für Datenschutz (ULD) alle Webseiten-Betreiber in Schleswig-Holstein aufgefordert, ihre Fanpages bei Facebook und Social-Plugins wie den „Gefällt mir-Button" auf ihrer Website zu entfernen. Der Düsseldorfer Kreis hat sich mit Beschluss vom 08.12.2011[95] weitgehend der Position des ULD angeschlossen. Der Düsseldorfer Kreis ist der Ansicht, dass in Deutschland ansässige Unternehmen, die durch das Einbinden von Social-Plugins wie etwa per Facebook Like-Button

[94] https://www.datenschutzzentrum.de/presse/20110819-facebook.htm
[95] http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/08122011DSInSozialenNetzwerken.html?nn=409242

auf sich aufmerksam machen oder sich mit Fanpages im Internet hervorheben wollen, grundsätzlich auch datenschutzrechtliche Verantwortung gegenüber dem Nutzer zu tragen haben. Entscheidend ist, dass beim Einbinden von Gefällt-mir-Buttons auf Webseiten schon beim Laden dieser Seite ohne Zutun des Nutzers Daten des Nutzers an den Betreiber der ggf. anzusprechenden Netzwerkplattform wie z. B. Facebook übertragen werden. Dieser erhält dann neben der URL der aktuellen Seite u. a. eine Kennung, die zumindest bei dort angemeldeten Nutzern direkt mit seiner Person verknüpft ist. Infolgedessen können durch die Betreiber der sozialen Netzwerke Surfprofile ihrer Nutzer erstellt werden.

Die Webseiten-Betreiber, die Social-Plugins einbinden, erheben selbst keine Daten oder speichern sie, „initiieren" aber die Datenweitergabe an z. B. Facebook, was man als einen datenschutzrelevanten Vorgang betrachten kann und wohl auch muss, denn er löst ohne weiteres Zutun des Betroffenen die Übertragung von dessen Daten an Dritte aus. Der Webseiten-Betreiber trägt daher hierfür die Verantwortung. Er muss deshalb die notwendigen Voraussetzungen schaffen und ggf. erforderliche Einwilligungserklärung des Nutzers einholen.

Die diesbezügliche Auffassung des ULD wie auch des Düsseldorfer Kreises erscheint daher zutreffend, auch wenn diese gelegentlich bestritten wird. Mittlerweile sind bei Verwaltungsgerichten Verfahren im Hinblick auf die Datenschutzkonformität des Unterhaltens von Facebook-Fanpages anhängig. Bis zu einer endgültigen Klärung wird empfohlen, das von Heise erarbeitete Konzept einer Zwei-Klick-Lösung zu etablieren, das auch von anderen Datenschutzaufsichtsbehörden anerkannt wird.

Dieses sieht vor, dass die Daten nur mit Zustimmung der Anwender übermittelt werden. Bei der Zwei-Klick Lösung werden standardmäßig nur „deaktivierte Buttons eingebettet, die keinen Kontakt mit den Servern von Facebook & Co. herstellen. Erst wenn der Anwender diesen Button aktiviert und damit seine Zustimmung zur Kommunikation mit Facebook, Google, Twitter oder anderen erklärt, werden die Buttons aktiv und stellen die Verbindung her. Dann kann der Anwender mit einem zweiten Klick seine Empfehlung übermitteln.

"[96]

Es wird in der nächsten Zeit zu beobachten sein, ob sich diese Zwei-Klick-Lösung etablieren lässt und somit tatsächlich eine Verbesserung der datenschutzrechtlichen Situation eintritt.

4.3.3 IP-Adressen als personenbezogene Daten

Die Frage, ob IP-Adressen personenbezogene Daten darstellen oder nicht, bewegte im Berichtszeitraum die Gemüter. Für meine Tätigkeit war zu entscheiden, ob IP-Adressen als personenbezogene Daten zu behandeln sind, was Folgen für deren Speicherung wie auch die Speicherfristen hat.

In Erwägungsgrund Nr. 26 zur EU-Datenschutzrichtlinie 95/46/EG wird eindeutig festgelegt, 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. Die europäische Artikel 29-Datenschutzgruppe hat dies in ihrem Arbeitspapier Nr. 159 besonders hervorgehoben.

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.[97] 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.[98]

[96] http://www.heise.de/ct/artikel/2-Klicks-fuer-mehr-Datenschutz-1333879.html
[97] vgl. Härting, Internetrecht, S. 22 Rdnr. 89
[98] vgl. Härting, CR 2008, S. 743, 745 f.

Nach § 3 Abs. 1 BDSG sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). 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 Bezug kennen, oder selbst herstellen können, oder es genügt, dass der Bezug ggf. auch nur von Dritten hergestellt werden kann, um auch die zu verpflichten, die dies aktuell nicht oder ggf. auch nur noch nicht können. Nach meiner Ansicht genügt, wie es auch das Gesetz ausdrückt, dass die betroffene Person bestimmbar ist. Die gegenteilige Meinung führt dazu, dass die betreffenden Daten solange völlig schutzlos und damit schrankenlos handelbar wären, bis sie endlich bei einer Person anlanden, der die Zuordnung konkret möglich ist. Dies würde zu einer erheblichen Gefährdung des Datenschutzes führen, die vom Gesetz nicht gewollt ist und sich durch eine Pseudonymisierung der erfassten Daten vermeiden lässt. Wer sich für die Person, die hinter einer dynamischen IP-Adresse steckt nicht interessiert, kann an Stelle der IP-Adresse ein beliebiges Pseudonym auswählen und speichern, das dann datenschutzrechtlich unproblematisch ist, gleichwohl aber den gleichen Zweck erfüllt.

Meiner Ansicht nach ist der absoluten Bestimmbarkeit der Vorzug zu geben. Auf diesen haben sich die Landesdatenschutzbeauftragten derzeit geeinigt.

4.3.4 Sonstige Anfragen

Eine allgemeine Anfrage betraf die Verweigerung von konkreten personenbezogenen Daten im Verwaltungsrechtsstreit. Diese Frage bezog sich auf einen konkreten Einzelfall.

Mit dem Bereich EDV wurden Fragen der Datensicherheit in einigen Zusammenhängen intensiv beraten.

Aus einem anderen Bereich ergaben sich Zweifelsfragen zur Zulässigkeit von Meinungsäußerungen in Internetforen, wobei diese sich inhaltlich auch mit Mitarbeitern der Landeszentrale auseinandersetzten.

Schließlich waren auch Datenschutzfragen im Zusammenhang mit der Zulässigkeit der Übermittlung von personenbezogenen Daten ehemaliger Mitarbeiter an potentielle neue Arbeitgeber im Ausland zu klären.

5. Datenschutz bei den Anbietern und Tochtergesellschaften der Landeszentrale

Einen maßgeblichen Teil meiner Tätigkeit bildete zudem 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.

Auffällig war die Anzahl der Beschwerden insbesondere wegen unerwünschter oder jedenfalls nicht erbetener Werbung per Post, E-Mail oder Telefon. Die Beschwerdeführer bemängelten nicht nur, dass sie diese Werbung 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 sowie der Übermittlung an Dritte ausgesprochen bzw. die Löschung aller gespeicherten Daten beantragt. Häufig schien dies den Beschwerdeführern ohne Einschaltung des Beauftragten für den Datenschutz bei der Landeszentrale in einer für sie akzeptablen Zeit nicht möglich zu sein.

Einige Fälle waren wieder auf eine Verwechslung von Daten bei Anbietern zurückzuführen. In anderen Fällen musste die Zulässigkeit des vorliegenden Handels mit Adressen zu Werbezwecken geprüft werden. Die einschlägigen Vorschriften hierzu wurden durch die BDSG-Novelle II vom 14.08.2009[99] erheblich verändert.

Im Jahr 2010 stieg die Anzahl der Beschwerden gegenüber den Vorjahren nochmals an. Häufig verfolgte eine große Anzahl der Beschwerden die Thematik der unzulässigen Datennutzung auch in der Form unerwünschter oder jedenfalls nicht erbetener Werbung per Post, E-Mail oder Telefon. Zu Überprüfen waren auch die Zulässigkeit von Bonitätsprüfungen sowie die Rechtmäßigkeit der Übermittlung der personenbezogenen Daten an Dritte. Darüber hinaus begehrten die Beschwerdeführer Auskunft über die Herkunft der Daten und deren Verwendungszweck. In der Regel wurde eine Löschung oder Sperrung der Daten und eine Bestätigung dieser Vorgänge gefordert, eine Untersagung der zukünftigen Speicherung ohne Genehmigung sowie der Übermittlung an Dritte ausgesprochen bzw. die Löschung aller gespeicherten Daten beantragt.

Auch im Jahr 2011 war weiterhin eine hohe Anzahl an Beschwerden zu bearbeiten, mit denen ähnlich Anliegen wie die vorgenannten verfolgt wurden; allerdings erreichten die die Anliegen zunehmend auch grundlegendere Fragestellungen, was inhaltlich häufig zu einem deutlich höherem Zeitaufwand in der Bearbeitung führte.

[99] Vgl. oben 2.3.1.1

Auffällig war, dass sich die Beschwerden auf mehr Angebotsformen von Rundfunk erstreckten als dies in früheren Jahren der Fall gewesen war; so richteten sich diese nicht nur oder weitestgehend auf Pay-TV Anbieter wie in den Vorjahren, sondern betrafen zunehmend auch Free-TV- und Radio-Anbieter sowie Internetradioanbieter. Die Themen reichten von der datenschutzrechtliche Überprüfung von Gewinnspielen der Anbieter bis hin zu datenschutzrechtlichen Fragestellungen im Bereich von deren Telemedien.

Eine Beschwerde richtete sich gegen die Ortung von Mobilfunkgeräten zur Erstellung und Übermittlung von Staumeldungen. Diese Frage sollte uns später noch einmal in im Rahmen einer Landtagspetition erreichen.

Im Rahmen des Internets ging es um die Einbindung von Anwendungen wie etwa den oben bereits angesprochenen Facebook Like-Button oder die erforderlichen Datenschutzerklärungen. Darüber hinaus war die ebenfalls schon dargestellte Problematik der Speicherung von IP-Adressen zu behandeln, wobei die bisher noch gesetzlich ungeschriebene Frist von sieben Tagen, die im Diskussionsentwurf des Bundesjustizministerium vom 07.06.2011[100] für ein „Gesetz zur Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdaten im Internet“[101] vorgesehen ist, einen gewissen Gestaltungsspielraum für die Praxis eröffnete.

Im Bereich der Beschwerden gegen Pay-TV Anbieter kamen neue Fragestellungen hinzu, wie z.B. die Versendung von Bankverbindungsdaten zu Prüfungszwecken. Problematische Vorgehensweisen wurden stets umgehend für künftige Vorgänge umgestellt, ohne dass es einer lückenlosen Ausräumung aller Gegenargumente bedurft hätte.

Im Sommer 2011 wurde dem Beauftragten für den Datenschutz seitens eines Anbieters ein Datenschutzvorfall gemeldet. Es ging um einen Hackerangriff auf Teilnehmerdaten eines kostenlosen Gewinnspiels. Nach dem Vorfall war die Aufsicht umgehend informiert und der Umstand ebenso den Teilnehmern mitgeteilt worden. Da keine besonderen personenbezogenen Daten i.S.d. § 3 Abs. 9 BDSG betroffen waren, handelte es sich nicht um eine Datenschutzpanne i.S.d. § 42 a Nr. 1 BDSG. Der Anbieter hat darüber hinaus alles Erforderliche veranlasst um eine weitere über die bereits entstandene hinaus gehende Gefährdung der Interessen der betroffenen Teilnehmer auszuschließen oder doch zumindest soweit als möglich zu minimieren und die Sicherheitslücke zu schließen. Besondere aufsichtliche Maßnahmen waren daher nicht veranlasst.

[100] Vgl. oben 2.2.3
[101] http://wiki.vorratsdatenspeicherung.de/images/DiskE_.pdf

Insgesamt konnten die an den Beauftragten für den Datenschutz herangetragenen Anfragen und Beschwerden in allen begründeten Fällen und nahezu vollständig im Sinne des jeweiligen Petenten geklärt bzw. dessen Anliegen Rechnung getragen werden, so dass trotz der deutlich angestiegenen Anzahl an Verfahren keine weitergehenden Konsequenzen im Sinne einer intensiveren aufsichtlichen Einwirkung auf einzelne Anbieter abgeleitet werden mussten.

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 zählte im Berichtszeitraum auch der regelmäßige Besuch der Sitzungen und Veranstaltungen der Gesellschaft für Datenschutz und Datensicherheit e.V. und hierbei insbesondere die Sitzungen des Erfa-Kreises Bayern, in denen einerseits ausgewählte Institutionen und Firmen in Vorträgen und Erfahrungsberichten ihre besondern Aufgabenschwerpunkte und die dabei zu beachtenden und zu bewältigenden datenschutzrechtlichen Herausforderungen vor- und zur Diskussion stellen. Andererseits werden in diesen Veranstaltungen auch allgemeine und spezielle datenschutzrechtliche Fragestellungen erörtert und von fachkundiger Seite über die aktuelle Rechtsentwicklung berichtet und diese fachlich bewertet.

Eine besondere Beachtung verdienen Veranstaltungen, die sich in verschiedenster Form und mit unterschiedlichen Aufgabenstellungen und Zielsetzungen in Fragen der Rechtsfortbildung und seit dem Ende 2011 verstärkt mit den Inhalten, Vorteilen und Schwächen und Folgewirkungen der EU-Datenschutz-Grundverordnung befassen.

Darüber hinaus wird laufend ein Erfahrungsaustausch mit dem Bayerischen Landesamt für Datenschutzaufsicht in Ansbach, und Kontakte zum Landesbeauftragten sowie zum für Datenschutzrecht zuständigen Referat des Staatsministeriums des Inneren gepflegt.

Im Herbst 2011 wurde in der Landeszentrale eine Sitzung des Erfa-Kreises ausgerichtet, in der ich einen Vortrag zum Thema „Datenschutz in Rundfunk und den neuen Medien“ hielt. Dargestellt wurden die aufsichtsrechtlichen Institutionen im Bereich des Bundes und der Länder im öffentlichen und nichtöffentlichen Bereich sowie die besonderen Zuständigkeiten in den Bereichen Kirche, Presse und Rundfunk und hierbei insbesondere die Bedeutung, Aufgabe und Rechtfertigung der rundfunkrechtlichen Datenschutzbeauftragten bei ARD, ZDF und der Landeszentrale.

Besonderes Interesse fanden die bis dahin weitgehend jedenfalls unbeachteten Auswirkungen, die sich aus dem nur im Rundfunkrecht üblichen Organisationsgrundsatz ergeben, dass die Rundfunkanbieter ein Wahlrecht hinsichtlich der sie beaufsichtigenden Instanz, also der zuständigen Landesmedienanstalt besitzen. Besonders plastisch werden die Folgen im Falle von Sendergruppen, die Genehmigungen für verschiedene Fernsehangebote von unterschiedlichen Landesmedienanstalten besitzen, so dass man für die unterschiedlichen Angebote dieser Gruppe zu völlig unterschiedlichen Zuständigkeiten gelangt.

Da die örtlichen Zuständigkeiten im Übrigen wie z.B. im Hinblick auf den Datenschutz im Allgemeinen wie auch in Bezug auf Telemedien am Sitz des Veranstalters anknüpfen, ergeben sich bei verschiedenen Kombinationen zum Teil durchaus überraschende Ergebnisse, die vor allem für betroffene Bürger zu jedenfalls für diese zumeist unlösbaren Fragen führen. Mit Blick auf das sich mit Spannung entwickelnde Thema HbbTV und die sich daran anschließenden konvergenten Entwicklungen dürften diese Fragen weiterhin zunehmend an Bedeutung gewinnen.

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 einerseits über einen besonderen Bezug zu und spezielle Kenntnisse von der Arbeit der Anbieter und ihren Umfeldbedingungen wie auch über eine intensive Erfahrung mit rundfunkrechtlichen Zusammenhängen und Fragestellungen verfügt, andererseits aber auch über die verfassungsrechtlich geforderte Unabhängigkeit, die den Rundfunkbereich insgesamt auszeichnet. Der Umstand, dass diese Konstruktion zumindest im Ergebnis unterdessen 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 auch im Rahmen meiner Tätigkeit erheblich an Bedeutung gewonnen hat, ist gerade aus diesem Bereich und insbesondere dem künftig im Rahmen der Konvergenz der Medien und Übertragungsnetze zu erwartenden deutlich intensiveren Zusammenspiel von Rundfunk und Telemedien ein neuer Schwerpunkt in meinem Tätigkeitsfeld zu erwarten, über welchen künftig zu berichten sein wird, und in welchem wohl auch Plattformen für Rundfunk- und Telemedien und ggf. auch Suchmaschinen und andere Netzwerke wegen ihrer Bedeutung für die Rundfunknutzung eine Rolle spielen dürften.