Bayerische Landeszentrale für neue Medien

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

(Berichtszeitraum: 01.01.2012 bis 31.12.2013)

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 elfte Tätigkeitsbericht seit Inkrafttreten des BayMG am 01.12.1992 und bezieht sich auf die Jahre 2012 und 2013.

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.

Besondere Aufmerksamkeit erforderte im Berichtszeitraum die Befassung mit bei Anbietern entstandenen Datenpannen. Das Thema Videoüberwachung gab Anlass zur intensiven Auseinandersetzung mit den datenschutzrechtlichen Vorschriften. Und schließlich entwickelt sich die Frage, welche Sicherheitsanforderungen sich aus Datenschutzvorgaben ergeben und wie hierauf im täglichen Umgang wie vor allem auch bei der Konzeptionierung von IT-Systemen zu reagieren ist, zu einem neuen Schwerpunkt in meiner laufenden Tätigkeit.

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

2. Entwicklung des Datenschutzrechts

2.1 Internationale Entwicklungen

Aufgrund der stetig wachsenden Internationalisierung der Weltwirtschaft 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.

Gerade in 2013 hat sich z.B. durch die von Edward Snowden enthüllte Prism-Affäre gezeigt, dass auch deutsche Staatsbürger von internationalen Vorgängen wie Spähattacken unmittelbar betroffen sein können. Wegen der technologischen Führerschaft der USA in IT-Fragen kommt dem US-amerikanischen Recht und den Rechtsbeziehungen zu den USA auch für die Europäer eine wachsende Bedeutung zu, die sich in der Intensität der Berichterstattung über das Verhältnis zu den USA wenn auch auf niedrigem Niveau in der täglichen Arbeit zeigt.

2.1.1 Beschluss des Düsseldorfer Kreises vom 11./12.09.2012: Datenübermittlung in Drittstaaten erfordert Prüfung in zwei Stufen[1]:

Nach § 4 b BDSG 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. 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[2].

In einer Studie zum Safe Habor Treatment von 2008[3] wurde kritisiert, dass nur ein geringer Teil der Organisationen, die diese Vorgaben anerkannt haben, diesen tatsächlich- entsprechen[4]. Nachdem auch der Düsseldorfer Kreis, der Zusammenschluss der obersten Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich, selbst ähnliche Feststellungen gemacht hatte, beschloss er am 29.04.2010, dass solange eine flächendeckende Kontrolle der Selbstzertifizierung US-amerikanischer Unternehmen durch die Kontrollbehörden in Europa und den USA nicht gewährleistet ist, deutsche Unternehmen die Verpflichtung trifft, gewisse Mindestkriterien selbst zu prüfen, bevor sie personenbezogene Daten in die USA übermittelt.[5]

Mit Beschluss vom 11./12.09.2013 entwickelte der Düsseldorfer Kreis diese Vorgaben dahingehend weiter, dass nun Datenschutzfragen bei Datenübermittlungen in einen Drittstaat, der außerhalb des Europäischen Wirtschaftsraums liegt, in zwei Stufen geprüft werden müssen.

"Auf der ersten Stufe ist erforderlich, dass die Datenübermittlung durch eine Einwilligung der betroffenen Person oder Rechtsvorschrift gerechtfertigt ist. Hierbei gelten die allgemeinen Datenschutzvorschriften (z.B. §§ 28 und 32 BDSG) mit der Besonderheit, dass trotz Vorliegens einer Auftragsdatenverarbeitung die Datenübermittlung nach § 4 Abs. 1 BDSG zulässig sein muss (vgl. § 3 Abs. 8 BDSG). Bei Auftragsdatenverarbeitung ist der Prüfmaßstab in der Regel § 28 Abs. 1 Satz 1 Nr. 2 BDSG, bei sensitiven Daten ist § 28 Abs. 6 ff. BDSG zu beachten.
Auf der zweiten Stufe ist zu prüfen, ob im Ausland ein angemessenes Datenschutzniveau besteht oder die Ausnahmen nach § 4c BDSG vorlie-

[1] http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/12092013DatenuebermittlungInDrittstaaten
[2] http://www.export.gov/safeharbor/eu/eg_main_018475.asp; diese wurden von der EG-Kommission am 26.07.2000 gebilligt und werden allgemein seit November 2000 praktiziert.
[3] Conolly, The US Safe Habor – Fact or Fiction? (2008), www.galexia.com
[4] Erd, Safe Habor Abkommen in K&R S. 626.
[5] Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 28./29.04.2010 in Hannover, S.1.

gen."[6]

Im Ergebnis ist eine Datenübermittlung folglich nur zulässig, wenn auf beiden Prüfstufen ein positives Ergebnis vorliegt.

2.1.2 Gesetzesvorhaben in den USA SOPA und PIPA[7] abgelöst durch CISPA

Die vormaligen Gesetzesentwürfe SOPA (Stop Online Piracy Act)[8] (ein Gesetzesentwurf vom 26. Oktober 2011, der im US-amerikanischen Repräsentantenhaus vom Abgeordneten Lamar Smith Republikanische Partei Texas) und PIPA ("Protect IP Act") (ein von den Demokraten im Senat eingebrachter Gesetzesvorschlag) wurden nunmehr durch einen neuen US-Gesetzesentwurf genannt "CISPA" abgelöst.

Nachdem Internetgiganten wie Wikipedia, Google, Facebook, Twitter und Ebay im Januar 2012 Protestaktionen starteten, weil sie aufgrund der Entwürfe zu einem Anti-Piraterie-Gesetz eine mögliche Zensur des Internets befürchteten, waren die Gesetzesvorhaben SOPA und PIPA gescheitert.

Nunmehr liegt seit 22.05.2012 der Gesetzesentwurf CISPA (Cyber Intelligence Sharing and Protection Act) "Kampf gegen Cyberbedrohung" vor[9].

Während SOPA es den Urheberrechtsinhabern ermöglichen sollte, die nicht genehmigte Verbreitung urheberrechtlich geschützter Inhalte durch gerichtliche Verfügungen gegen Internetseiten wirksam zu verhindern, hat CISPA einen anderen Anwendungsbereich. Zweck von CISPA ist es, den Informationsaustausch zwischen US-Firmen und US-Behörden zur Bekämpfung von Cybercrime zu fördern. Zudem kann CISPA nicht auf Urheberrechtsverletzungen angewendet werden.[10]

CISPA wurde zwar am 26.04.2012 im Repräsentantenhaus beschlossen, nicht aber im US-Senat.[11] Nachdem die Berater des US-Präsident Obama der Ansicht waren, dass der Gesetzentwurf die Privatsphäre und bürgerlichen Freiheiten schwäche, rieten sie diesem sein Veto einzulegen.[12] Allerdings hat das Repräsentantenhaus den Gesetzentwurf im Februar 2013 erneut eingebracht und verabschiedete diesen dann am 18. April 2013[13].

---

[6] S.o. Fn. 1.
[7] Quelle: http://de.wikipedia.org/wiki/Stop_Online_Privacy_Act
[8] Bill Text, 112th Congress (2011-2012), H.R.3261.IH
[9] http://web.archive.org/web/20120522154416/http://www.rules.house.gov/Media/file/PDF_112_2/LegislativeText/CPRT-112-HPRT-RU00-HR3523.pdf
[10] Vgl. MMR-Aktuell 2012, 331642.
[11] http://clerk.house.gov/evs/2012/roll192.xml
[12] http://www.bbc.com/news/world-us-canada-17864539
[13] http://clerk.house.gov/evs/2013/roll117.xml

Der Senat hat den Entwurf am 22. April 2013 erhalten, jedoch nicht beschlossen. Am 10. Juli 2014 wurde dem Senat ein ähnliches Gesetz (CISA) vorgestellt. Der Gesetzesentwurf CISPA wurde am 8. Januar 2015 schließlich noch einmal in das Repräsentantenhaus eingebracht und ist bis dato immer noch nicht beschlossen[14].

2.1.3 Transatlantischen Handels- und Investitionspartnerschaft (TTIP)[15]

Die EU und die USA besprechen sich bereits seit 2011 über ein Handelsabkommen, das seit 2013 konkret diskutiert wird. Ziel der TTIP ist es, die Vorschriften und Regeln in der Wirtschaft Europas und den USA langfristig so gestalten, dass sie besser miteinander vereinbar sind. Die Verbraucher ebenso wie die Unternehmen hätten durch gemeinsame Standards bei Zukunftstechnologien Vorteile. Im Jahr 2013 und 2014 gab es mehrere Verhandlungsrunden. Für Februar 2015 ist eine weitere geplant.

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

Der Datenschutz wird durch TTIP bei der handelsbezogenen Kommunikation betroffen.

Die allgemeinen transatlantischen Datenschutzfragen sollen wie bisher in Freihandelsverhandlungen und den dafür vorgesehenen Gremien und Regelwerken (etwa der Ad-hoc Expertengruppe EU-US Working Group on Data Protection oder der EU-US-Safe-Harbor-Vereinbarung) gelöst werden.

Sofern der Datenschutz etwa auch handelsbezogene Kommunikation, wie bei Dienstleistungen im IKT-Bereich und bei E-Commerce betrifft, werden solche Aspekte im Rahmen von TTIP behandelt werden. Auf die derzeitig laufenden Verhandlungen zur EU-Datenschutzreform hat das TTIP jedoch keinen Einfluss.

Der Information des BMWi ist zu entnehmen: "Generell setzt sich die Bundesregierung für hohe Datenschutzstandards auch im transatlantischen Verhältnis ein. Die bestehenden Datenschutzstandards in Deutschland und der EU stehen nicht zur Disposition."[16]

[14] http://en.wikipedia.org/wiki/Cyber_Intelligence_Sharing_and_Protection_Act
[15] http://www.bmwi.de/DE/Themen/Aussenwirtschaft/Ttip/faqs.html
[16] http://www.bmwi.de/DE/Themen/Aussenwirtschaft/Ttip/faqs.html

2.1.4 ACTA – Anti-Counterfeiting Trade Agreement

Das "Anti-Piraterie-Abkommen" ACTA[17] war als ein multilaterales Handelsabkommen auf völkerrechtlicher Ebene geplant, und sollte internationale Standards im Kampf gegen Produktpiraterie und Urheberrechtsverletzungen schaffen. Während der ersten ohne Information der Öffentlichkeit stattfindenden drei Jahre dauernden Verhandlungen vertrat die Europäische Kommission die EU-Mitgliedstaaten. Nach Protesten von Bürgerrechtlern wurde im April 2010 eine umfassende Dokumentation auf der Internetseite der Kommission zur Verfügung gestellt[18].

Anfang 2012 hatten neben zahlreichen Staaten wie z.B. Kanada, Australien, Japan, und den USA auch 22 der 27 EU-Mitgliedstaaten das Abkommen unterzeichnet. Deutschland hatte aus formalen Gründen und wohl auch, weil die damalige Bundesjustizministerin Sabine Leutheusser-Schnarrenberger die Unterschrift ablehnte, noch nicht unterschrieben.

Nach offiziellen Informationen war das Ziel lediglich die Bekämpfung organisierter Urheberrechtsverstöße; es gehe nicht darum die täglichen Nutzungsgewohnheiten im Internet zu beschränken. Es sollten keine Internetseiten geschlossen werden können. Es würden auch keine Endgeräte überprüft; ACTA sei nicht Big Brother. Alles was bisher legal sei, wäre auch nach der Ratifizierung noch legal.[19]

Diese Einschätzung wurde jedoch nicht überall geteilt. Der Bundesbeauftragte für Datenschutz und Informationsfreiheit teilt in seinem Tätigkeitsbericht 2009/2010[20] mit, dass bei der Beratung des Abkommens unter anderem davon die Rede gewesen sei, TK-Anbieter mit Blick auf Urheberrechtsverstöße zur Überwachung ihrer Kunden zu verpflichten. Da dies eine anlasslose Speicherung von IP-Adressen und TK-Verkehrsdaten mit sich bringe, wäre derartiges unter dem Gesichtspunkt einer möglichen Vorratsdatenspeicherung zweifelhaft.

Aber auch Stimmen aus der Wirtschaft[21] äußerten sich kritisch, weil Internetprovider ggf. nur dann haftungsfrei blieben, wenn sie die komplette Kommunikation ihrer Nutzer überwachten und Urheberrechtsverstöße dann direkt gegenüber dem Nutzer ahnden würden, ggf. bis hin zur Kündigung des Internetanschlusses. Daher wurde auch kritisiert, dass das Abkommen den Rechtsstaat in Richtung zur Zensur beschneide, weil einschneidende Maßnahmen ohne gerichtliche Verfahren getroffen würden.

---

[17] Rat der Europäischen Union, institutionelles Dossier: 2011/0166 (NLE), letzter Stand vom 09.09.2011, 12196/3/11 REV 3 (de).
[18] http://ec.europa.eu/trade/creating-opportunities/trade-topics/intellectual-property/anti-counterfeiting/
[19] S.o. Fn. 14.
[20] Tätigkeitsbericht des Bundesbeauftragten für Datenschutz und Informationsfreiheit 2009/2010, S. 52.
[21] Bericht im Handelsblatt vom 25.01.2012.

Nach einer reichhaltigen öffentlichen Diskussion wurde schließlich das Abkommen im Europaparlament am 04.07.2012 mit großer Mehrheit (478 gegen 39 bei 165 Enthaltungen) abgelehnt. Danach dürfte das Abkommen zumindest derzeit in Europa kaum Chancen auf Verwirklichung haben.[22]

2.2 Europäisches Recht

Das nationale Datenschutzrecht ist zunehmend durch Vorgaben der Europäischen Union geprägt. Den grundlegenden Rahmen geben bisher die EU-Datenschutzrichtlinie[23] sowie die E-Privacy-Richtlinie (RL 2002/58/EG)[24] 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 mit sich. Durch ihn werden die bislang geltenden Gemeinschaftsverträge grundlegend umgestaltet. Eine entscheidende Neuerung ist die Aufhebung der Säulenstruktur[25] und die Einbindung der Charta der Grundrechte in das europäische Primärrecht. Für den Datenschutz ergeben sich daraus nicht unerhebliche Folgerungen.

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

- Mit dem Wegfall der bisherigen Säulenstruktur wird der bisher der dritten Säule zugehörende Bereich der zwischenstaatlichen polizeilichen- und justiziellen Zusammenarbeit "vergemeinschaftet" und un-

[22] http://www.heise.de/newsticker/meldung/EU-Parlament-beerdigt-ACTA-1632071.html
[23] RL 95/46/EG, ABl. EG v. 23.11.1995, Nr.L 281/31.
[24] Im Telekommunikationsbereich wird die Datenschutzrichtlinie durch die im Jahr 2002 erlassene RL 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) ergänzt.
[25] Die Europäische Union bestand bis zum Inkrafttreten des Vertrages von Lissabon aus dem Bereich der Europäischen Gemeinschaften (1. Säule), der gemeinsamen Außen- und Sicherheitspolitik (2. Säule) und der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (3. Säule).
[26] Vertrag über die Arbeitsweise der Europäischen Union.
[27] Vgl. unten 2.2.2.

terliegt nunmehr grundsätzlich auch dem Geltungsbereich des Art. 16 AEUV.

Am 27. November 2008 hat der Rat der EU-Innen- und Justizminister einen Rahmenbeschluss über den Datenschutz in der dritten Säule verabschiedet.[28] Ob dieser den Anforderungen des Art. 16 AEUV entspricht, wurde kontrovers diskutiert, da er 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 auch die Ausgestaltung hinsichtlich des Rechtes des Betroffenen auf Auskunft empfunden, weil diese den Mitgliedsstaaten überlassen wurde.

- Die wohl wichtigste Änderung ist jedoch die Bezugnahme auf die Charta der Grundrechte im Vertrag von Lissabon. In **Art. 8 der Grundrechtecharta**[29] ist ein **Grundrecht auf Datenschutz** normiert, das zum ersten Mal auf europäischer Ebene rechtsverbindlich gilt. Was dies für die Geltung deutscher Grundrechte bedeutet, insbesondere ob die europäischen Grundrechte ein vergleichbares Schutzniveau gewährleisten[30], ist ebenso umstritten wie die zu erwartenden Folgen einer diese ausgestaltenden EU-Datenschutz-Grundverordnung. Der für Datenschutzfragen bisher zuständige Bundesverfassungsrichter Prof. Masing[31] vertritt in einer öffentlichen Stellungnahme die Auffassung, dass mit einer solchen Verordnung wohl auch deutsches Verfassungsrecht verdrängt würde, so dass die das Datenschutzrecht bisher maßgeblich im Sinne eines effektiven Grundrechtsschutzes prägende Rechtsprechung des Bundesverfassungsgerichtes dann weitgehend bedeutungslos würde.

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.[32] Am 25. Januar 2012 hat die Europäische Kom-

[28] ABl. EU 2008/L 350/60.
[29] Artikel 8 Schutz personenbezogener Daten
(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.
[30] Vgl. *Ronellenfitsch,* Der Vorrang des Grundrechts auf informationelle Selbstbestimmung vor dem AEUV, DuD, 2009, S. 451 ff.
[31] Johannes Masing, "Ein ‚Abschied von den Grundrechten", SZ 29.01.2012.
[32] http://www.statewatch.org/news//2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf

mission den Entwurf einer europäischen Datenschutz-Grundverordnung[33] offiziell vorgelegt, der seither im Europäischen Parlament und im Rat intensiv erörtert wird.

Die Datenschutz-Grundverordnung soll die bisherige EU-Datenschutzrichtlinie 95/46/EC ersetzten und nach dem derzeitigen Stand wohl den Datenschutz im gesamten öffentlichen und nichtöffentlichen Bereich mit nur geringen Ausnahmen regeln. Von der Datenschutzgrundverordnung wären somit die Landeszentrale selbst ebenso wie auch die bei ihr genehmigten Anbieter unmittelbar betroffen.

Zentrales Anliegen der Datenschutzgrundverordnung 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 28 Mitgliedsstaaten angleichen soll. 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, die Bedeutung der europäischen Datenschutzvorgaben ggf. auch weltweit zu erhöhen und für eine größere Wettbewerbsgleichheit zwischen europäischen und außereuropäischen Unternehmen auf dem europäischen Markt aber auch darüber hinaus zu sorgen.

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

[33] 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.

zentralen Punkten massiv behindert würde.

Zudem würden die entgegenstehenden 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 wohl ausscheiden dürften. Allenfalls könnte ein Verstoß gegen europäische Grundrechte vorliegen, der beim EuGH zu rügen wäre. Dass es dort jedenfalls bisher keine dem BVerfG entsprechende Expertise in Sachen Grundrechtsschutz gibt, wäre dann ein Umstand, an den man sich jedenfalls für einige Zeit 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, dass die Bedeutung von personenbezogenen Daten heute immer nur in der individuellen Nutzungssituation und im konkreten Einzelfall bewertet werden kann. Das deutsche Datenschutzrecht kennt daher auch nur eine Hervorhebung von Daten als besonders sensibel[34]; 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

[34] Vgl. § 3 Abs. 9 BDSG.

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. Zudem bestehen erhebliche Zweifel an der technischen Umsetzbarkeit.

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 in zahllosen Vorschriften die Zuständigkeit der EU-Kommission für **Delegierte Rechtsakte** vor, so dass die Kommission in diesen Materien die Befugnis zum Erlass von weiteren Vorschriften erhalten würde, die die zumeist allgemein gehaltenen Vorgaben der Datenschutz-Grundverordnung als europäisches recht konkretisieren würden. Diese Rechtsakte würden bereits wirksam, sofern das EU-Parlament nicht innerhalb von zwei Monaten Einwände erhebt.

2.2.2.3 Verfahrensstand

Das Europäische Parlament hat zu Stellungnahmen aufgefordert und unzählige Änderungsvorschlägen erhalten. Der federführende Berichterstatter Jan Philipp Albrecht (Fraktion Gründe/EFA) legte im Januar 2013 seinen darauf aufbauenden Entwurf mit zahlreichen Änderungsvorschlägen und politisch wünschenswerten Postulaten vor. Im Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres (LIEBE) des Europäischen Parlaments wurde dieser letztlich weitgehend akzeptiert und zum Ende der letzten Legislaturperiode auch vom Europaparlament angenommen, so dass dieser Entwurf wohl den Parlamentsvorschlag im Rahmen eines künftige Triloges darstellen wird.

Der Rat der Europäischen Union (Rat für Justiz und Inneres) beriet parallel dazu, konnte bisher aber die erforderliche Einigung nur zu einigen Kapiteln herstellen, so dass dessen Beratung und Abstimmung noch andauert.

2.2.2.4 Bewertung des Vorhabens

Dem Gesetzgebungsvorhaben liegen viele sinnvolle Überlegun-

gen und Zielsetzungen zugrunde, wie die Stärkung der Datenschutzrechte der Bürger, die Geltung europäischen Rechtes für Datenverarbeitungsvorgänge in Europa und bezüglich der Daten von Europäern und langfristig auch die Schaffung eines einheitlichen Datenschutzniveaus in Europa. Die dafür vorgesehene Datenschutz-Grundverordnung enthält auch zweifellos viele gute Ansätze. Daneben hält sie auch zahlreiche Anreize für zahlreiche Gruppen von Betroffenen bereit.

Ob sich die so geweckten Erwartungen aber mit einer Datenschutzgrundverordnung werden letztlich verwirklichen lassen, erscheint durchaus zweifelhaft; ja es erscheint sogar keineswegs als ausgeschlossen, dass insbesondere für die Bürger anstelle der geplanten und angepriesenen Vorteile tatsächlich eher Nachteile entstehen, sei es z.B. durch ein Absenken des Datenschutzniveaus oder durch nachhaltige Rechtsunsicherheit, weil das neue Recht in vieler Hinsicht neue Fragen aufwirft, diese aber nicht hinreichend konkret beantwortet. Hinzu kommt, dass die Datenschutzgrundverordnung einen sehr weiten Anwendungsbereich haben soll, da sie für alle Bürger und alle Unternehmen in den meisten Lebenssituationen und nun wohl auch wieder für alle staatlichen Institutionen gelten soll. Dass eine solche "Herkules-Aufgabe" in vergleichsweise kurzer Zeit sinnvoll zu bewältigen sein könnte, erscheint jedenfalls sehr ambitioniert bis nahezu ausgeschlossen.

Auch der Umstand, dass die Datenschutzgrundverordnung ein einheitliches Datenschutzniveau verspricht, bisher aber keine tragfähigen Lösungen für eine Umsetzung in der Praxis enthält, spricht gegen den Ansatz der Verordnung. Einerseits beschränken sich zahlreiche Vorgaben letztlich auf die Durchführung einer Güterabwägung, die naturgemäß in 28 EU-Mitgliedsstaaten mit höchst unterschiedlicher Datenschutztradition und abweichenden Wertvorstellungen[35] nicht einheitlich ausfallen kann. Andererseits muss nach Art. 16 Abs. 2 AEUV wie auch Artikel 8 EU-Grundrechtecharta die Einhaltung dieser Vorschriften von unabhängigen Stellen überwacht werden, was die von der Kommission vorgesehene eigene Vorrangstellung wohl ausschließt, aber auch verbindliche Abstimmungsprozesse unter den Datenschutzaufsichtsinstitutionen problematisch erscheinen lässt.

[35] Man denke z.B. nur an den Umstand, dass man in London nahezu überall einer Videoüberwachung ausgesetzt ist, und dies dort auch allgemein akzeptiert wird, während dies in Deutschland eher wohl nicht der Fall wäre, vgl. Carsten Knop in FAZ vom 10.02.2015 S. 15.

Ob die bisher vorgesehene Datenschutzgrundverordnung in ihrer jetzigen Form die mit ihr verbundenen Nachteile wirklich aufwiegen kann, erscheint zweifelhaft. Dies gilt insbesondere auch für die vom Prof. Masing[36] angesprochenen zu erwartenden Folgewirkungen für die künftige Geltung und Bedeutung des nationalen Verfassungsrechts.

Um einerseits die zweifelsfrei guten und unterstützenswerten Grundüberlegungen umzusetzen, andererseits aber auch die o.g. Nachteile zu vermeiden, sollte die Planung einer umfassenden Datenschutzgrundverordnung aufgegeben werden und anstelle dessen eine Umsetzung der inhaltlichen Planungen in der Form einer **Kombination aus Richtlinie und Verordnung** präferiert werden. Dies würde einen deutlich flexibleren Weg eröffnen, der dem in letzter Zeit wieder stärker betonten Subsidiaritätsprinzip[37] wie auch den sehr unterschiedlichen Historien in den Mitgliedsstaaten der EU deutlich besser gerecht würde.

Bei dieser Lösung würden nur diejenigen Bestandteile der Planungen in einer europäischen Verordnung unmittelbar und ohne Ausführungsspielräume der nationalen Gesetzgeber vorgeschrieben werden, die dieser Rechtsqualität unbedingt bedürfen, zudem aber auch mit solcher Klarheit erlassen werden können, dass eine unmittelbar geltende europäische Regelung angemessen erscheint.

Die übrigen Materien, die dies nicht erfordern bzw. bei denen der europäische Gesetzgeber sich ohnehin noch nicht auf hinreichend klare Regelung festlegen möchte oder konnte, würden wie bisher in der Form einer Richtlinie beschlossen, die Mindeststandards für die Ausgestaltung des Datenschutzes in allen EU-Mitgliedsstaaten festschreibt. Bei Richtlinien sind derartige Unschärfen und Spielräume üblich, und werden dem Subsidiaritätsprinzip folgend durch nationales Recht ausgefüllt und konkretisiert. Eine solche Konzeption wäre flexibler, dürfte schneller einigungsfähig sein und beschlossen werden können, und würde die Stärken des Ansatzes umsetzbar machen, ohne die Schwächen in Kauf nehmen zu müssen und sollte daher vorzugswürdig sein.

2.2.3 Zulässigkeit der Vorratsdatenspeicherung

[36] Johannes Masing, "Ein ‚Abschied von den Grundrechten", SZ 29.01.2012.
[37] BRat Drs. 52/12 v. 30.03.2012; der Bundesrat hat bereits mit seiner Subsidiaritätsrüge am 29.03.2012 eine entsprechende Stellungnahme abgegeben.

Mit der Richtlinie 2006/24/EG[38] des Europäischen Parlaments und des Rates vom 15. März 2006 wurden die EU-Mitgliedsstaaten verpflichtet dafür Sorge tragen, dass von Anbietern von Telekommunikationsdiensten Verbindungsdaten mindestens sechs Monate auf Vorrat gespeichert werden, Art. 3 i.V.m Art. 6 RL.

Die Kategorien der zu speichernden Daten waren in Art. 5 RL beschrieben und umfassten etwa bei Telefongesprächen die Telefonnummer, Namen und Anschrift sowie den Zeitpunkt und Dauer des Gesprächs. Bei der Nutzung von Mobilfunkgeräten kamen Funkzelle, Identifikationsnummer und geografische Ortung, bei der Internetnutzung Benutzerkennung und IP-Adressen und beim E-Mailverkehr Kontaktdaten und Zeiten der Internetnutzung hinzu.

Die gegen diese Richtlinie gerichteten Klagen von Irland und der Slowakei wurden am 10. Februar 2009 vom EuGH[39] zurückgewiesen, der entschied, dass die Richtlinie (2006/24/EG) auf der Grundlage des EG- Vertrages wirksam erlassen worden sei. Der EuGH stellte hierbei aber auch klar, dass die Entscheidung keinerlei Aussage zu einer möglichen Verletzung der Grundrechte durch die Richtlinie in materieller Hinsicht treffe, sondern

[38] ABl. EG v. 15.03.2006, Nr. L 105/54.
[39] EuGH Urt. v. 10.02.2009, Az: C-301/06.

sich lediglich auf die richtige Wahl der Rechtsgrundlage beziehe.[40]

In Deutschland wurde das die Richtlinie umsetzende Gesetz am 09.11.2007 im Bundestag verabschiedet und am 26.12.2007 vom Bundespräsidenten unterzeichnet[41]. Es trat am 01.01.2008 in Kraft und wurde durch das Bundesverfassungsgericht mit Urteil vom 02.03.2010[42] als mit dem Grundgesetz unvereinbar verworfen.[43]

Aufgrund von Meinungsverschiedenheiten innerhalb der damaligen Bundesregierung war es seither zu keiner Neuregelung gekommen[44]. Der im Dezember 2013 vereinbarte Koalitionsvertrag von CDU, CSU und SPD sah dann vor, dass die EU-Richtlinie zur Vorratsdatenspeicherung umgesetzt werde, um Zwangsgelder zu vermeiden. "Dabei sollte ein Zugriff auf die gespeicherten Daten nur bei schweren Straftaten und nach Genehmigung durch einen Richter sowie zur Abwehr akuter Gefahren für Leib und Leben erfolgen."[45]

Am 12.12.2013 stellte der Generalanwalt beim EuGH in seinen Schlussanträgen fest, dass die Richtlinie zur Vorratsdatenspeicherung gegen die EU-Grundrechtecharta verstoße[46]. Daraufhin kündigte Bundesjustizminister Maas im Januar 2014 an, keinen Gesetzesentwurf zur Umsetzung der Richtlinie vorzulegen, ehe eine endgültige Entscheidung des EuGH ergangen sei[47]. Im April 2014 entschied der EuGH, dass die Richtlinie tatsächlich gegen die EU-Grundrechtecharta verstoße[48]. Damit sind jedenfalls zunächst alle bisherigen Planungen obsolet.

---

[40] Der EuGH hielt es für gerechtfertigt, dass der Gemeinschaftsgesetzgeber das Ziel, das Funktionieren des Binnenmarkts zu schützen, durch den Erlass von solchen Harmonisierungsvorschriften verfolge.
Warum eine solche Verpflichtung wirklich für das Funktionieren des Binnenmarktes erforderlich sein soll, wurde nicht begründet. Zudem harmonisierte die Richtlinie keineswegs nur Speicherungspflichten, sondern führte massiv in die Datenschutzrechte der Gemeinschaftsbürger eingreifende Verpflichtungen auch für die Länder verbindlich ein, in denen es bis dahin keine derartige Verpflichtung gab und in denen zudem berechtigte Zweifel bestanden, ob deren nationale Gesetzgeber eine solche Verpflichtung überhaupt einführen könnten, geschweige denn würden.

[41] "Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer versteckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG", BGBl I 2008, S. 70.

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

[43] Das Gericht war der Ansicht, der Gesetzgeber sei seinem Auftrag nicht nachgekommen, "die Ermächtigung zur Massenspeicherung von Telekommunikationsdaten mit angemessenen Schutzmechanismen zu flankieren, weshalb die momentane deutsche Umsetzung der Richtlinie verfassungswidrig und nichtig sei", vgl. K&R 2010, S. 220.

[44] Vgl. Möstl, Zeitschrift für Rechtspolitik 2011, S. 226.

[45] Koalitionsvertrag 16.12.2013, S. 102, 103.

[46] Vgl. Roßnagel MMR 2014, Editorial 73.

[47] Vgl. Roßnagel K&R 2014, Editorial 74.

[48] Vgl. EuGH Urt. v. 08.04.2014 K&R 2014, 405 ff.

2.2.4 Richtlinie 2009/136/EG[49]

Am 25.11.2009 haben das Europäische Parlament und der Rat der Europäischen Union mit der Richtlinie 2009/136/EG verschärfte Informationspflichten für den Fall einer Verletzung des Schutzes personenbezogener Daten geschaffen. Nach dem neuen Art. 4 Abs. 3 der E-Privacy-Richtlinie[50] hat der Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste im Falle einer Verletzung des Schutzes personenbezogener Daten unverzüglich die zuständige nationale Behörde und darüber hinaus auch die betroffenen Personen von der Verletzung zu benachrichtigen, wenn anzunehmen ist, dass diese durch die Verletzung des Schutzes personenbezogener Daten in ihrer Privatsphäre beeinträchtigt werden.

Diese Informationspflicht ist weitergehender als die bisher[51] vorgesehenen und erfasst nicht nur unrechtmäßige Übermittlungen mit der Folge schwerwiegender Beeinträchtigungen, sondern jede Art von Sicherheitsverletzung, die auf unbeabsichtigte oder unrechtmäßige Weise zur Vernichtung, zum Verlust oder zur Veränderung der Daten führt. Die Diensteanbieter werden zudem verpflichtet, ein Verzeichnis der Verletzungen des Schutzes personenbezogener Daten zu führen. Die Umsetzung[52] der Richtlinie erfolgte in der Novelle zum TKG vom 09.05.2012[53].

Zudem enthält diese RL 2009/136/EG aber auch die Vorgabe[54], künftig eine Speicherung von Informationen oder den Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, im Wesentlichen nur zu gestatten, wenn der betreffende Teilnehmer oder 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. Erfolgt ist die Umsetzung jedoch bis heute nicht. Der seinerzeitige Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Schaar hielt daher die E-Privacy-Richtlinie insoweit in Deutschland für unmittelbar anwendbar.

2.3 Bundesrecht

[49] 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.
[50] Datenschutzrichtlinie für elektronische Kommunikation, RL 2002/58/EG.
[51] Z.B. in § 42a BDSG, § 15a TMG und § 93 Abs. 3 TKG.
[52] Die eigentliche Frist zur Umsetzung in nationales Recht lief bis zum 25.05.2011.
[53] BGBl. I 2012, S. 958.
[54] Über eine Änderung von Art. 5 Abs. 3 der RL 2002/58/EG, der sog. E-Privacy-Richtlinie.

2.3.1. Bundesdatenschutzgesetz (BDSG)

2.3.1.1 Beschäftigtendatenschutz

Zum Arbeitnehmerdatenschutz wurde im August 2010 ein Gesetzesentwurf[55] vorgelegt. Danach sollte der bisherige § 32 BDSG entfallen und der Beschäftigtendatenschutz umfassend in den neuen Vorschriften der §§ 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 05.11.2010 zum Gesetzesentwurf Stellung[56], das Gesetz wurde jedoch bis zum Ende der letzten Legislaturperiode nicht verabschiedet.

Im Koalitionsvertrag einigten sich dann CDU, CSU und SPD darauf, die Verhandlungen zur Europäischen Datenschutzgrundverordnung insoweit mit dem Ziel zu verfolgen, das vorhandene nationale Datenschutzniveau zu erhalten und über das Europäische Niveau hinausgehende Standards zu ermöglichen. Nur sofern mit dem Abschluss der Verhandlungen über die Europäische Datenschutz-Grundverordnung nicht in angemessener Zeit zu rechnen sei, wolle man eine nationale Regelung zum Beschäftigtendatenschutz schaffen.[57]

2.3.1.2 Rote-Linie-Gesetz[58]

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. 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 In-

[55] Gesetzesentwurf Bundesregierung; BR-Drs. 535/10.
[56] Stellungnahme BR-Drs. 535/10.
[57] Koalitionsvertrag v. 16.12.2013 S. 50.
[58] http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/rote_linie.pdf?__blob=publicationFile

ternetdiensten, die für die Integrität der Persönlichkeitsrechte von besonderer Bedeutung sind, wie Gesichtserkennungsdienste oder Dienste zur Profilbildung. Den Betroffenen soll künftig bei schweren Verletzungen des Persönlichkeitsrechts ein immaterieller Schadensersatzanspruch zustehen.
Die eingeleitete Resort Abstimmung zu dem Gesetzesvorhaben wurde im Februar 2011 unterbrochen und ist bisher noch nicht abgeschlossen. Sollte eine solche Regelung jedoch kommen, hätte sie gerade für den Medienbereich erhebliche Bedeutung.

2.3.2 Telekommunikationsgesetz (TKG)

Im Jahr 2012 waren die EU-Richtlinien 2009/140/EG[59] und 2009/136/EG[60] umzusetzen. Dies erfolgte mit Gesetz vom 03.05.2012[61], das die folgenden datenschutzrechtlich bedeutsamen Änderungen zur Folge hatte:

- In § 91 Abs. 1 TKG wurde der Anwendungsbereich auf Telekommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen, erweitert, womit insbesondere RFID[62]-Geräte gemeint sind.[63] Diese finden vielseitige Verwendung und werden von der Fahrzeugsicherung über die Warenflusskontrolle, Transport und Logistik bis zu Gebrauchsgütern des täglichen Bedarfs eingesetzt. Dementsprechend wächst die Bedeutung von RFID für den Bürger.
- § 92 TKG wurde gestrichen. Die Übermittlung personenbezogener Daten ins Ausland ist seither in den §§ 4b und 4c BDSG abschließend geregelt.[64]
- 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.[65] Nach § 98 Abs. 1 Satz 1 TKG dürfen Standortdaten ohne Einwilligung des Teilnehmers nur anonym erhoben werden.
- In § 108 TKG werden neue Sicherheitsanforderungen und Benachrichtigungspflichten für den Notruf vorgegeben.

2.3.3 Telemediengesetz (TMG)

[59] RL 2009/140/EG, ABl. L 337 v. 18.12.2009, 37.
[60] RL 2009/136/EG, ABl. L 337 v. 18.12.2009, 11.
[61] BGBl. 2012 I 2012, S. 958.
[62] Radio Frequency Identification Devices.
[63] Roßnagel/Johannes/Kartal, Die TK-Novelle, K&R 2012, S. 250.
[64] Roßnagel/Johannes/Kartal, Die TK-Novelle, K&R 2012, S. 250.
[65] Roßnagel/Johannes/Kartal, Die TK-Novelle, K&R 2012, S. 250.

Daneben hätte auch die Richtlinie 2009/136/EG [66] und die darin enthaltene Änderung des Art. 5 Abs. 3 der E-Privacy-Richtlinie (2002/58/EG), die den Einsatz von Cookies beschränkt und ihren Gebrauch von der vorherigen Einwilligung des Nutzers abhängig macht, bis zum Mai 2011 umgesetzt werden müssen.[67] Hierzu hatte der Bundesrat am 17.06.2011 einen Gesetzesentwurf beschlossen[68], der umfangreiche Änderungen im TMG, insbesondere zusätzliche Pflichten für Anbieter von Telemedien mit nutzergenerierten Inhalten vorsieht[69].

Die Bundesregierung war 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 Fragen auf, die zunächst zu klären wären, was aber bisher nicht gelang. Dies könnte möglicherweise mit zu erwartende EU-Datenschutz-Grundverordnung[70] und deren künftigem Geltungsbereich im Zusammenhang stehen.

2.3.4 Entwurf eines IT-Sicherheitsgesetzes

Das Bundesministerium des Inneren veröffentlichte am 05.03.2013 den Entwurf des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG), das Änderungen am bestehenden BSI-Gesetz[71] mit dem Ziel vorsieht, digitale Netzwerke innerhalb Deutschlands wirksamer zu schützen. Der Entwurf des Gesetzes entstand bereits vor Bekanntwerden der NSA-Affäre, erhielt dadurch aber eine zusätzliche Brisanz. Der Gesetzesentwurf enthält u.a. eine Meldepflicht bei IT-Sicherheitsvorfällen. Wegen der mit den Sicherheitsmaßnahmen verbundenen Kosten wie auch der zu erwartenden Kontrollen der Netzwerke traf das Vorhaben auf nicht unerheblichen Widerstand. Im Berichtszeitraum kam es zu keiner abschließenden Beschlussfassung. Am 18.08.2014 [72] wurde ein neuer Referentenentwurf vorgelegt, der nun beraten wird.

---

[66] S.o. Fn. 49.
[67] S.o. 2.2.4
[68] BR Drs. 156/11.
[69] So sollen z.B. die Informationspflichten der Diensteanbieter gegenüber den Nutzern verstärkt werden, Datenschutzhinweise sollen in allgemeinverständlicher Form, leicht erkennbar und unmittelbar erreichbar sein. Es soll für Nutzer jederzeit und ohne technisches Hintergrundwissen die Möglichkeit bestehen, datenschutzrechtliche Informationen zu erhalten. Standardmäßig sollen bei Neuanmeldungen zunächst die höchsten Sicherheitsstufen voreingestellt sein, die nur vom Nutzer gelockert werden können, und es soll eine wichtige Voreinstellung geben, die die Auffindbarkeit und Auslesbarkeit mittels externer Suchmaschinen verhindert. Zudem sollen die Nutzer durch Aufklärung hinsichtlich der Risiken der Veröffentlichung persönlicher Daten sensibilisiert werden. Letztlich soll der Nutzer immer die Gelegenheit haben, seine in dem Telemediendienst veröffentlichten Daten wieder zu löschen oder zumindest zu sperren oder zu anonymisieren.
[70] vgl. Art. 89 EU-Datenschutzgrundverordnung (Entwurf der EU-Kommission) der das künftige Zusammenspiel mit der E-Privacy-Richtlinie (2002/58/EG) wohl nur scheinbar klar regelt.
[71] BSI-Gesetz v. 14.08.2009 (BGBL. I, S. 2821).
[72] http://www.computerundrecht.de/Entwurd_IT-Sicherheitsgesetz_1808.pdf

2.3.5 Entwurf eines Gesetztes zur Strafbarkeit der Datenhehlerei (§ 202d StBG)

Im Zuge der vorgenannten Diskussion um ein Sicherheitsgesetz wurde bereits im Juni 2013 vom Bundesrat ein Gesetzesentwurf zur Strafbarkeit der Datenhehlerei[73] vorgelegt. Der Bundesrat trägt in seinen Entwurf vor, dass mit der sich rasant entwickelnden Informationstechnologie der Handel mit rechtswidrig erlangten digitalen Daten wie z.B. Kreditkartendaten oder Zugangsdaten zum Onlinebanking, E-Mail-Diensten oder sozialen Netzwerken immer mehr an Umfang gewonnen habe.

Die Täter würden häufig selbst keine unmittelbaren Vermögensverfügungen vornehmen, sondern über Webportale auf intensive Weise Handel mit den ausgespähten Daten betreiben. Da die mit Bereicherungs- und Schädigungsabsicht vorgenommene Weitergabe nur in Teilbereichen von bestehenden Strafnormen gedeckt sei, könne man bisher dem massenhaften Missbrauch nicht ausreichend begegnen.

Der Schutz des Bürgers ergebe sich aus dem "Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme"[74]. Zur wirksamen Bekämpfung der Cyberkriminalität sieht der Gesetzentwurf konsequenterweise auch eine Erhöhung der Strafrahmen für das Ausspähens und Abfangens von Daten (§§ 202a, 202b StGB) vor.

2.3.6 Allgemeines Gleichbehandlungsgesetz (AGG)

Das allgemeine Gleichbehandlungsgesetz wurde zwar im Berichtszeitraum verändert[75]. Diese Änderungen haben jedoch für den Datenschutz keine Bedeutung, so dass insoweit auf den 10. Tätigkeitsbericht verwiesen werden kann.

[73] 07.06.2013 (BR-Drs. 284/13 [B].
[74] BVerfGE 120, 274 ff.
[75] AGG zuletzt geändert durch Art. 8 G v. 3.4.2013 I 610.

2.3.7 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)[76] beschlossen. Das Gesetz trat am 01.01.2010 in Kraft. Dadurch wurden die Arbeitgeber gesetzlich verpflichtet, monatlich entsprechende Meldungen an die zentrale Speicherstelle über Gehaltszahlungen wie auch über Schwankungen des regelmäßigen Gehaltes und die hierfür maßgeblichen Gründe abzugeben. Als besonders problematisch wurden Angaben über krankheits- oder gar arbeitskampfbedingte Gründe angesehen.

Datenschützer hatten während des gesamten Entstehungsprozesses massive Bedenken angemeldet, weil Daten mit einer erheblichen Detailtiefe zentral, anlasslos und sogar auch zu Personen erhoben werden sollten, bei denen es zumindest als sehr unwahrscheinlich erschien, dass die Daten tatsächlich jemals gebraucht würden.

Am 31.03.2010 wurde Verfassungsbeschwerde gegen den elektronischen Einkommensnachweis ELENA in Karlsruhe eingereicht. Nach einer eingehenden politische Diskussion wurde in einer gemeinsamen Presseerklärung des Bundesministeriums für Wirtschaft und Technologie und des Bundesministeriums für Arbeit und Soziales vom 18.07.2011[77] mitgeteilt, dass man sich nach eingehender Überprüfung des ELENA-Verfahrens geeinigt habe, dieses schnellstmöglich einzustellen. Mit dem Gesetz vom 23.11.2011[78], das zum 01.01.2012 in Kraft trat, wurde das ELENA-Verfahren eingestellt.

2.3.8 Bundesmeldegesetzes

Die Bundesregierung hat zum 31.08.2011 einen Gesetzentwurf zum Melderecht in Deutschland beschlossen. Dadurch sollten erstmals bundesweit einheitliche und unmittelbar geltende melderechtliche Vorschriften für alle Bürger und Bürgerinnen geschaffen werden. Der Bundestag beriet am 26.04.2012 über den Gesetzesentwurf in erster Lesung.[79] In zweiter und dritter Lesung wurde der Gesetzesentwurf am 28.06.2012 – wohl vor leeren Parlamentssitzen während eines EM-Fußball-Halbfinalspieles[80] – beschlossen. In dieser Fassung war es den Meldebehörden erlaubt, persönliche Daten von Bürgern an Firmen zu verkaufen, sofern nicht ausdrücklich ein Widerspruch der Betroffenen vorliegt. Daran entzündete sich eine öf-

[76] BGBl. I 2009, S. 634 f.
[77] http://www.bmwi.de/DE/Presse/pressemitteilungen,did=424742.html
[78] Gesetz zur Änderung des Beherbergungsstatistikgesetzes und des Handelsstatistikgesetzes sowie zur Aufhebung von Vorschriften zum Verfahren des elektronischen Entgeltnachweises, BGBl. 2011, S. 2299.
[79] http://www.bmi.bund.de/SharedDocs/Standardartikel/DE/Themen/OeffentDienstVerwaltung/Meldewesen/ausblick.html
[80] Vgl. Abel, Das neue Melderecht, RDV 2013, S. 179.

fentliche Diskussion über die Weitergabe von Meldedaten an Dritte.

Der Bundesrat rief am 21.09.2012 den Vermittlungsausschuss an, in dem sich Bund und Länder einigten, die Notwendigkeit der Einwilligung wieder einzuführen. Das Bundesmeldegesetz wurde am 28.02. bzw. 01.03.2013 beschlossen und am 08.05.2013 [81] verkündet. Danach ergeben sich folgende Neuregelungen:

- Soweit Melderegisterauskünfte zur gewerblichen Nutzung erfragt werden, ist zukünftig der Zweck der Anfrage anzugeben und die Melderegisterauskunft ausschließlich zu diesem Zweck zu verwenden.

- Melderegisterauskünfte 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 erhalten rund um die Uhr länderübergreifend einen Online-Zugriff auf die Meldedaten.

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

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

- Eine Evaluation der neuen Regelungen durch die Bundesregierung auf wissenschaftlicher Grundlage und anschließende Berichterstattung an Bundestag und Bundesrat vier Jahre nach Inkrafttreten des Gesetzes."[82]

2.4 Länderübergreifende Anwendungshinweise für die Nutzung von personenbezogenen Daten für werbliche Zwecke[83]

Seit dem Jahr 2013 dient der Düssendorfer Kreis als Gremium in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder der Kommunikation, Kooperation und Koordinierung der Aufsichtsbehörden im nicht-öffentlichen Bereich[84]. Der Düsseldorfer Kreis hatte eine Arbeitsgruppe "Werbung und Adresshandel" unter Leitung des Bayerischen Landesamts für Datenschutzaufsicht eingerichtet und diese mit der Erarbeitung von Anwendungshinweisen zu den BDSG-Regelungen für den werblichen Umgang mit personenbezogenen Daten

[81] BGBl. I S. 1084.
[82] http://www.bmi.bund.de/DE/Themen/Moderne-Verwaltung/Verwaltungsrecht/Meldewesen/Bundesmeldegesetz/bundesmeldegesetz_node.html
[83] http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/Anwendungshinweise_Werbung.pdf
[84] http://de.wikipedia.org/wiki/D%C3%BCsseldorfer_Kreis

beauftragt. Die Anwendungshinweise wurden im Dezember 2013 veröffentlicht.[85]

Diese behandeln detailliert nahezu alle relevanten datenschutzrechtlichen aktuellen Fragen im Zusammenhang mit Werbemaßnahmen und geben Hinweise für eine datenschutzkonforme Durchführung. Dabei werden auch Verknüpfung zum Wettbewerbsrecht hergestellt was diese Anwendungshinweise als für die Praxis besonders hilfreich erscheinen lässt.

Sie befassen sich beispielsweise mit den Voraussetzungen für Werbemaßnahmen hinsichtlich der Einwilligung im Sinne des § 4a BDSG unter Berücksichtigung der dazu ergangenen BGH-Rechtsprechung und der Empfehlungen der Art. 29-Datenschutzgruppe[86] oder mit Listendaten und deren Nutzungsdauer aus rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnissen.

2.5 Bayerisches Landesrecht

2.5.1 Änderung des BayDSG

Das BayDSG hat im Jahr 2012 einige Änderungen erfahren, welche ihre Grundlage in Änderungen der Abgabenordnung, der Gewerbeordnung, des Sozialgesetzbuch X, des Telekommunikationsgesetz, des Bayer. Gesetz über das Erziehungs- und Unterrichtswesen, des Polizeiaufgabengesetzes und des Bayer. Statistikgesetz haben.

Die Änderungen des Jahres 2013 beruhten auf Bundesrechtsänderungen in der Abgabenordnung, der Gewerbeordnung, dem Sozialgesetzbuch X, dem Telekommunikationsgesetz, dem Strafgesetzbuch und der Strafprozessordnung sowie auf Veränderungen des Bayerischen Landesrechts im Verbraucherschutzgesetz, im Meldegesetz, im Bayer. Personalvertretungsgesetz, im Bayer. Rettungsdienstgesetz und im Bayer. Verfassungsschutzgesetz.

2.5.2 Rundfunkstaatsvertrag

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

2.5.3 Rundfunkgebührenstaatsvertrag

Der 15. Rundfunkänderungsstaatsvertrag wurde von den Regierungschefs am 15. – 21.12.2010 unterzeichnet und fristgemäß zum 31.12.2011 von

[85] S.o. Fn. 83
[86] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_de.pdf

den Länderparlamenten ratifiziert. Er trat am 01.01.2013 in Kraft[87].

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. Gleiches gilt für den Beitrag pro Betriebsstätte, der aber nach Anzahl der Mitarbeiter gestaffelt ist.

Hinsichtlich der Frage, ob bei diesem neuen Ansatz auch die Belange des Datenschutzes hinreichend berücksichtigt wurden, existierten nicht unerhebliche Auffassungsunterschiede. Während die Landesbeauftragten für den Datenschutz eklatante Normdefizite beklagten, waren die Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio der Auffassung, dass durch die Änderungen sogar eine Verbesserung des Datenschutzes einträte, da Nachforschungen beim betroffenen minimiert würden und sich der Einsatz von Rundfunkgebührenbeauftragten deutlich reduzieren lasse. Künftig würden weniger Daten erhoben, da die Angaben zu Art und Anzahl der bereitgehaltenen Geräte entfallen könnten, und da die Beitragspflicht nicht mehr von den persönlichen Lebensverhältnissen abhängig sei.

Auch der einmalige Meldedatenabgleich mit ca. 70 Mio übermittelten Datensätzen, der es anlässlich der Systemumstellung möglich machen sollte, die bisher nicht erfassten Beitragsschuldner zu ermitteln, wurde eher positiv bewertet, da die Datenerhebung bei einer Vielzahl von Beitragsschuldnern dadurch entbehrlich würde und nach Feststellung eines Beitragsschuldners die Daten der übrigen dort wohnenden Personen gelöscht werden könnten, sobald das Beitragskonto ausgeglichen sei. Insgesamt würden somit nur die Daten Zahlungspflichtiger langfristig gespeichert werden[88].

Die in "Zentraler Beitragsservice" umbenannte GEZ führt seit 2013 den Datenabgleich mit den Meldeämtern durch und verschickt an die bisher nicht gemeldeten Wohnungen Anfragen, ob die Anmeldung notwendig sei. Die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder angemahnte Nachbesserung der Staatsvertragsregeln zur Beachtung der Erforderlichkeit, Verhältnismäßigkeit, Normklarheit und Datensparsamkeit ist vom Gesetzgeber bisher nicht für erforderlich gehalten worden.

2.5.4 Bayerisches Mediengesetz

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

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

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

3. Funktion des Beauftragten für den Datenschutz

Mit Art. 20 BayMG als bereichspezifischer Datenschutznorm hat der Gesetzgeber das aus den verfassungsrechtlichen Vorgaben der Rundfunkfreiheit resultierende Gebot der Staatsferne der Landeszentrale auch für den Bereich des Datenschutzes umgesetzt. Diese gesetzgeberische Gestaltung, die einerseits der Rechtsprechung des Bundesverfassungsgerichts zum Recht auf informationelle Selbstbestimmung Rechnung trägt und andererseits ausdrücklich das Medienprivileg aufnimmt, hat sich nachhaltig bewährt.

Durch den Beauftragten für den Datenschutz bei der Landeszentrale können die spezifischen Anforderungen im Bereich des in öffentlich-rechtlicher Trägerschaft betriebenen Rundfunks gewährleistet werden, da 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[89], und zwar auch, soweit es sich um Verwaltungsangelegenheiten handelt.[90] Mit dieser umfassenden Zuständigkeit für alle Aufgaben bei der Landeszentrale und den Anbietern trägt das BayMG den verfassungsrechtlichen Anforderungen an einen rundfunkrechtlichen Datenschutz Rechnung.[91]

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.[92] 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 al-

---

[89] 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.

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

[91] 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."

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

lem im Hinblick auf die Überwachung der Datenschutzregelung nach Art. 20 Abs. 2 BayMG für den journalistisch-redaktionellen Bereich notwendig aber auch 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 des Europarechtes[93] einschließlich der EU-Datenschutzrichtlinie[94], die in Art. 28 Abs. 1 den Mitgliedsstaaten auferlegt, datenschutzrechtliche Kontrollstellen zu schaffen, die die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahrnehmen. Die sich aus dieser Vorgabe ergebenden Folgerungen waren in der Vergangenheit nicht unumstritten. Durch das Urteil des Europäischen Gerichtshofs vom 09.03.2010[95] wurden diese Zweifel ausgeräumt. Die Gestaltung nach dem BayMG entsprach diesen Vorgaben seit jeher.

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.[96]

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

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.

---

[93] Art. 8 Abs. 3 EU-Grundrechtecharta wie auch Art. 16 Abs. 2 AEUV sehen eine Beaufsichtigung durch unabhängige Stellen zwingend vor.
[94] RL 95/46/EG, ABl. EG v.23.11.1995, Nr. L 281/31.
[95] EuGH Urt. v. 09.03.2010, C- 518/07.
[96] Vgl. Art. 20 Abs. 3 Satz 1 BayMG.

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.

im Jahr 2012 wurde vom Bereich Kommunikation und Medienwirtschaft die Internetseite "Medienpuls" zur datenschutzrechtlichen Überprüfung vorgelegt. Gemeinsam mit dem Bereich Geschäftsleitung/IT wurden offene Fragen eingehend erörtert und die Ausgestaltung entsprechend datenschutzkonform 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 IT-Abteilung vereinbart, dass dieses Anlageverzeichnis in gewisser Weise fortgeführt wird. Ein Verwaltungsaufwand entsteht hierdurch nicht, da die eingesetzte Hardware sowie die Peripherie-Geräte weiter inventarisiert und als Anlagevermögen aktiviert 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 seit längerem als gelöst angesehen werden.

Nennenswerte Auffälligkeiten konnten im Berichtszeitraum nicht festgestellt werden.

4.3 Anfragen aus der Landeszentrale

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

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

Nach einer weiteren Zunahme der internen Anfragen im Jahr 2012 hat sich deren Anzahl im Jahr 2013 wieder auf dem Niveau von 2011 eingependelte. Allerdings nimmt die Komplexität der Fragen mit fortschreitender Digitalisierung aller Ar-

beitsprozesse zu und erhöht die Anforderungen.

4.3.1 Informationsaustausch und aktuelle Vorgänge

Mit der Geschäftsleitung findet regelmäßig i.d.R. vierteljährlich ein Informationsaustausch statt, in dessen Rahmen die allgemeinen den Datenschutz in der Landeszentrale betreffenden Fragen erörtert werden.

Darüber hinaus werden spezielle Fragen aus den Bereichen, gelegentlich aber auch der Geschäftsleitung zu Datenschutzfragen ggf. auch jenseits des unmittelnbaren Zuständigkeitsbereiches der Landeszentrale bearbeitet und geklärt.

Im Berichtszeitraum gehörten hierzu z.B. Fragen zu internationalen Entwicklungen wie der EU-Datenschutz-Grundverordnung[97] und dem ACTA-Anti-Counterfeiting Trade Agreement vom 3. Dezember 2010[98] sowie von außereuropäischen Vorgängen in USA betreffend SOPA und PIPA[99].

Hierzu zählen aber auch banal anmutende Alltagsfälle. Z.B. wird selbst die Landeszentrale nicht von unerwünschter Werbung verschont, die obendrein auch noch zur werblichen Ansprache personenbezogene Daten von herausgehobenen Mitarbeitern verwendet, was wohl die mit den Schreiben verfolgten Intentionen befördern und den Eindruck der Schreiben verstärken soll. Auch hier helfen datenschutzrechtliche Erwägungen rechtmäßige Verhältnisse herzustellen.

4.3.2 Auftragsdatenverarbeitung

Da sich in der Landeszentrale immer wieder Konstellationen ergeben, bei denen externe Unternehmen im Auftrag der Landeszentrale tätig werden und dabei personenbezogene Daten verarbeiten, kommt auch den in dieser Hinsicht geltenden datenschutzrechtlichen Regeln eine Bedeutung für die Tätigkeit der Landeszentrale zu.

Wie bereits im letzten Tätigkeitsbericht ausgeführt wurde, hat der Bundesgesetzgeber vor kurzem einen 10 Punktekatalog zur Auftragsdatenverarbeitung in das BDSG eingeführt, die unmittelbar nur für den nichtöffentlichen Berich gilt. Zwar wurde die Parallelvorschrift des Art.6 BayDSG nicht in gleicher Weise erweitert; dennoch wird Art. 6 BayDSG so ausgelegt, dass auch für den öffentlichen Bereich 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

[97] Vgl. oben 2.2.2.
[98] Vgl. oben 2.1.4.
[99] Vgl. oben 2.1.2.

BayDSG zur Überprüfung heranzuziehen.

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 die Zulässigkeit von deren Speicherung wie auch die dabei geltenden 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.[100] 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.[101]

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. 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 und des dahinterstehenden Grundrechtsschutzes führen, die vom Gesetz nicht gewollt ist und sich durch eine Pseudonymisierung der erfassten Daten vermeiden lässt. Wer sich für die Person, die

[100] Vgl. Härting, Internetrecht, S. 22 Rdnr. 89.
[101] Vgl. Härting, CR 2008, S. 743, 745 f.

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. Auf diese Sichtweise haben sich auch die Landesdatenschutzbeauftragten jedenfalls im Ergebnis geeinigt.

Im Jahr 2014 hat der BGH [102] die Frage, ob dynamische IP-Adressen personenbezogene Daten sind, dem EuGH zur Klärung vorgelegt. Der BGH möchte wissen, ob es sich bei den dynamischen IP-Adressen dann um personenbezogene Daten im Sinne des Art. 2 lit. a RL 95/46/EG handelt, wenn nicht der Diensteanbieter selbst, sondern ein Dritter das Wissen über die Identifizierung des Betroffenen verfügt[103]. Falls der EuGH dies bejaht, will der BGH zudem wissen, ob Art. 7 lit. f RL 95/46/EG der Regelung des § 15 Abs. 1 TMG entgegensteht, wonach die sogenannten Nutzungsdaten erhoben und verwendet werden dürfen, um die Inanspruchnahme von Telemedien zur ermöglichen und abzurechnen.

Der EuGH wird sich nun mit dieser Frage zu befassen haben und die Sichtweise des Europarechtes klarstellen. Da der EuGH seit geraumer Zeit auch die EU-Grundrechtecharta als Prüfungsmaßstab berücksichtigt, wird auch diese grundrechtliche europäische Position in die Abwägung einfließen.

Darüber hinaus werden in Deutschland aber auch die Vorgaben des Grundgesetzes bei dieser Frage für deutsche Behörden und Gerichte zu berücksichtigen sein, denn vom Personenbezug dieser Daten hängt häufig die Anwendbarkeit aller Datenschutzregeln für ganze Datenbestände aus Nutzungszusammenhängen ab; denn häufig ergibt sich der Personenbezug jedenfalls zunächst nur aus der gespeicherten IP-Adresse, zu der dann aber zahlreiche für sich nicht individualisierbare Zusatzinformationen hinzugespeichert werden. Insofern wirkt die IP-Adresse in diesen Fällen wie die Eintrittskarte in den Bereich des Datenschutzes, was natürlich auch aus der Sicht des Grundgesetzes zu bewerten sein wird.

Diese gilt auch für den Datenschutz im Hinblick auf alle Anwendungen im Zusammenhang mit HbbTV, denn auch hier wird sich eine Individualisierung der gewonnen Nutzungsdaten in erster Linie an einer Speicherung der IP-Adresse festmachen lassen, auch wenn sich unterdessen wohl immer klarer abzeichnet, dass eine Individualisierung von Geräten über die bei diesen vorgenommenen Browsereinstellungen wohl in ähnlicher Weise weltweit eindeutig möglich ist.

Ggf. wird sich der Streit in naher Zukunft auch dadurch erledigen, dass

[102] BGH 28.10.2014 VI ZR 135/13, NJW 2015, 368.
[103] MMR-Aktuell 2014, 363599.

technisch anstelle der bisher eingesetzten Version IPv4 das IPv6 (Internet Protocol Version 6) eingeführt wird, das dann wieder so viele IP-Adressen zur Verfügung stellt, dass mit der Einführung des neues Standards problemlos allen Rechnern und mobilen Engeräten eigenständige IP-Adressen statisch zugeordnet werden können. Spätestens dann dürfte der Personenbezug von IP-Adresse als Streitpunkt erledigt sein.

4.3.4 Zugriffsrechte auf E-Mail-Accounts und Ordner

Aktuelle Frage stellten sich immer wieder zum Umgang mit BLM-E-Mail-Accounts, die den Mitarbeitern individuell zugewiesen sind, wenn diese aus dem Dienst bei der Landeszentrale ausscheiden. Einen entscheidenden Gesichtspunkt bildete hier vor allem der Umstand, dass den Mitarbeitern die private Nutzung erlaubt ist, sich auf dem Account daher zumindest potentiell dienstliche wie auch private Mails befinden können.

Weiterhin stellten sich Fragen und waren Rückfragen zu den Zugriffs-, Lese- und Nutzungsrechten auf Ordnern im Netzwerk der Landeszentrale zu klären. Hierbei spielte auch eine Rolle, ob und wenn ja in welchem Umfang ein Zugriff auf BLM-Ordner im Netzwerk auch Tochtergesellschaften eingeräumt werden kann und zulässig ist.

Grundsätzlich ist hierbei immer darauf hinzuweisen, dass das deutsche Recht kein Konzernprivileg kennt, also auch in einen Konzern integrierte, ggf. sogar vollständig kontrollierte aber rechtlich selbständige Einheiten als Dritte angesehene werden, sodass Datentransfers gleich welcher Art in der Regel als Übermittlung an Dritte angesehen werden, die nur eingeschränkt zulässig sind[104].

Zudem ist auch innerhalb interner Einheiten einerseits auf die Datensparsamkeit zu achten und andererseits nur denjenigen Personen Zugriff zu Daten und Akten zu gewähren, denen eine Aufgabe übertragen wurde, zu deren Erfüllung diese Person den Zugang zu diesen Informationen benötigt (Art. 17 BayDSG).

4.3.5 Übermittlung von personenbezogenen Daten an Dritte

Immer wieder werden Anfragen gestellt, welche Daten z.B. von Anbietern bei Anfragen Dritter an diese Dritten übermittelt werden dürfen.

Hier ist der Standpunkt des Gesetzes wie auch der Landeszentrale sehr klar. Personenbezogenen Daten sind zu schützen; um solche (im Sinne des Art. 4 BayDSG) handelt es sich nur bei Daten, die sich auf natürliche

[104] S. unten 4.3.5.

Personen beziehen, nicht hingegen bei Daten einer juristischen Person. Sofern es jedoch um Daten geht, die sich zwar vordergründig auf eine juristische Person beziehen, darüber hinaus aber durchaus auch Aussagen über die "dahinterstehenden" natürlichen Personen enthalten, kann ein Personenbezug vorliegen, der den Schutzbereich des Datenschutzes eröffnet[105]. Häufig liegen solche Gestaltungen bei OHG's, KG's, nichtrechtsfähigen Vereinen oder "Einmann-GmbHs" vor, so dass Aussagen über die dortigen z.B. finanziellen Verhältnisse auch einen Rückschluss auf die Kreditwürdigkeit des Gesellschafters-Geschäftsführers als natürliche Person ermöglichen können.

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

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

[105] Vgl. Komm. z. BayDSG, Wilde, Ehmann, Niese, Knoblauch, 20. Ergänzungslieferung, Stand April 2014, Art. 4 Rdnr: 11.

4.3.6 Zweckfremde Verwendung von Bestandsdaten

Ein weiterer Dauerbrenner sind die Nachfragen zur Verwendung von Bestandsdaten, die die Landeszentrale zumeist auf ganz unterschiedliche Weise und in unterschiedlichen Zusammenhängen erhalten hat.

Die Verarbeitung und Nutzung von personenbezogenen Daten ist gemäß Art. 17 Abs. 1 BayDSG nur zulässig, soweit es zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich ist und die Verarbeitung und Nutzung für die Zwecke erfolgt, für die die Daten erhoben worden sind. Auch für den Fall, dass keine Erhebung vorausgegangen ist, weil die personenbezogenen Daten freiwillig abgegeben wurden, dürfen die Daten nur zu dem Zweck geändert oder genutzt werden, für den sie gespeichert wurden.

Die personenbezogenen Daten, zu denen in der Regel auch E-Mail-Adressen zählen, dürfen gem. Art. 17 Abs. 2 Nr. 2, Nr. 3 BayDSG für einen anderen Zweck genutzt werden, sofern der Betroffene eingewilligt hat, oder offensichtlich ist, dass die Zweckänderung in seinem Interesse liegt, und kein Grund zu der Annahme besteht, dass er in Kenntnis des anderen Zweckes seine Einwilligung hierzu verweigern würde.

Die Zweckänderung muss im objektiven Interesse des Betroffenen liegen; er darf durch die Zweckänderung keine Nachteile zu erwarten haben und es dürfen keine Anhaltspunkte dafür vorliegen, dass der Betroffene seine Einwilligung verweigern würde [106].

Im Einzelfall kann man wohl davon ausgehen, dass es z.B. im Interesse von Teilnehmern von Veranstaltungen liegt, die im Zusammenhang mit einer Veranstaltung der Landeszentrale ihre Daten hinterlassen haben, über weitere Veranstaltungen der Landeszentrale informiert zu werden. Soll hier Klarheit geschaffen werden, kann das in der Regel nur über eine Einwilligung erfolgen, die im Vorfeld entsprechend den dafür geltenden Regelungen - z.B. bereits auf der entsprechenden Website durch ein Opt-In-Feld - eingeholt wird.

4.3.7 Nutzungsbedingungen für den Einsatz von mobilden Endgeräten

Im Zuge der Einführung neuer mobiler Geräte in der Landeszentrale, waren auch datenschutzrechtliche Belange bei der Erstellung der Nutzungsbedingungen zur Verwendung der neuen I-Phones und I-Pads zu dienstlichen Zwecken mit zulässiger Privatnutzung zu berücksichtigen. Die dabei vorgetragenen Gesichtspunkte wurden in die "technischen und organisa-

[106] Vgl. Fn. 105, Wilde/Ehmann/Niese/Knoblauch, Art. 17 Rn. 21.

torischen Nutzungsbedingungen für den Einsatz von mobilen Endgeräten (iPhones, iPads)" aufgenommen, die so auch datenschutzrechtliche Fragen umfassen und die Nutzung dieser Geräte in dieser Hinsicht absichern.

5. Datenschutz bei den Anbietern und Tochtergesellschaften der Landeszentrale

5.1 Allgemeines

Einen maßgeblichen Teil meiner Tätigkeit bildete wie auch in den Vorjahren die Beratung der Anbieter in Fragen des Datenschutzes und insbesondere hinsichtlich der sich aus den gesetzlichen Vorgaben ergebenden Anforderungen für die Gestaltung des betrieblichen Ablaufs. Dabei erforderte das Thema Videoüberwachung im Geschäftsbetrieb von Anbietern wie auch die Bewältigung von Datenlecks im Berichtszeitraum besondere Aufmerksamkeit.

Inzwischen gehört die Bewältigung einer großen Anzahl von Beschwerden insbesondere wegen unerwünschter oder jedenfalls nicht erbetener Werbung per Post, E-Mail oder Telefon inhaltlich zu den Routineaufgaben, die aber durch die im Jahr 2013 nochmals deutlich anstiegene Anzahl dennoch eine erhebliche Herausforderung darstellten. Die Beschwerdeführer bemängelten nicht nur, dass sie 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 wie auch der Übermittlung an Dritte ausgesprochen bzw. die Löschung aller gespeicherten Daten beantragt.

Zumeist waren die Beschwerdeführern durchaus zunächst im unmittelbaren Kontakt mit den betroffenen Anbietern; häufig konnten die Beschwerdeführern ihre in der Regel berechtigten Anliegen aber nicht oder jedenfalls nicht in einer ihnen akzeptabel erscheinenden Zeitspanne durchsetzen, so dass sie sich zur Einschaltung des Beauftragten für den Datenschutz bei der Landeszentrale veranlasst sahen.

Wie bereits erwähnt, bildete häufig eine unzulässigen Datennutzung für Werbezwecke den unmittelbaren Anlass für Beschwerden. Zu überprüfen waren aber beispielsweise auch die Zulässigkeit von Bonitätsprüfungen oder die Rechtmäßigkeit der Weitergabe von Daten an Dritte bis hin zu behauptetem unzulässigem Datenhandel sowie die Verknüpfung mit weiteren Rechtsgeschäften wie z.B. Abonnements.

In der Regel konnte dem Beschwerdevorbringen in einem überschaubaren Zeitraum abgeholfen und die begehrte Löschung bzw. Sperrung von Daten bewirkt oder die gewünschte Auskunft bzw. Bestätigung des Bestehen oder Nichtbestehens eines Rechstverhältnisses beigebracht werden.

5.2 Anfragen und Petitionen zu Hörfunkprogrammen

Aufgrund von Beschwerden und einer Landtagsanfrage hatten wir uns mit Fragen zur Zulässigkeit der Durchführung von Telefonumfragen wie auch der möglichen Ortung von Mobilfunkgeräten und der Nutzung dieser Daten zum Zwecke der Erstellung und Übermittlung von Staumeldungen zu befassen.

Zur Frage, ob das Ankündigen und Durchführen von **telefonische Umfragen** durch **Radiostationen** datenschutzrechtlichen Bedenken begegnet, war grundsätzlich auszuführen, dass aufgrund des § 30a BDSG das geschäftsmäßige Erheben und Speichern von Daten unter den dort genannten Voraussetzungen für Zwecke der Markt- und Meinungsforschung erlaubt ist. Solche Umfragen sind prinzipiell möglich und zulässig. Daher hat die Landeszentrale zulässigerweise wie in den Vorjahren die Konzeption des Beteiligungs- und Finanzierungsmodells für die rund 80 Auftraggeber der Studie "Funkanalyse Bayern" ausgearbeitet. Die beteiligten Anbieter hatten dabei die Möglichkeit, ihre Anforderungen an das Erhebungsmodell und die inhaltliche Ausgestaltung der Funkanalyse Bayern einzubringen. Dass Radiosender auf die Durchführung der oben genannten Studie hinweisen, um die Hörer über den Zweck der Umfrage zu informieren, ist aus datenschutzrechtlicher Sicht unbedenklich.

Hinsichtlich der Frage, ob **Radiostationen Handyortungen verwenden** dürfen, um den Verkehrsfluss anzusagen, war zunächst festzustellen, dass Radiostationen keine Sonderstellung genießen, sondern an die in diesem Bereich geltenden allgemeinen Gesetze gebunden sind. Soweit personenbezogene Daten genutzt werden sollen, ist dies nur mit Einwilligung der Betroffenen oder aufgrund einer gesetzlichen Bestimmung zulässig.

Ein praktischer Anwendungsfall, der bekannt wurde, beruhte auf folgenden Fakten: Ein Sender arbeitete bei der Beschaffung von aktuellen Verkehrsmeldungen mit einem Anbieter von Navigationslösungen und standortbezogenen Diensten zusammen, um die Hörerinnen und Hörer noch besser über die aktuelle Verkehrslage zu informieren und rechtzeitig vor Staus zu warnen. Der Sender nutzte gebrauchsfertige "Verkehrsflussdaten" des Dienstleisters, die aufgrund von ausgewerteten GPS und GSM-Daten gewonnen werden. Der Sender hatte dabei keinen Zugriff auf den Server des Dienstleisters und wertete selbst keine Handy-Daten aus. Senderseitig werden somit keinerlei personenbezogenen Daten gespeichert, verarbeitet oder genutzt. Der fragliche Dienstleister unterliegt jedoch nicht der Zuständigkeit des Beauftragten für den Datenschutz; es wurde aber versichert, dass er die vorgegebenen Datenschutzregeln einhalte. Anhaltspunkte für einen datenschutzrechtlichen Verstoß waren daher nicht zu erkennen.

5.3 Arbeitnehmerdatenschutz und Videoüberwachung

Aufgrund von Arbeitnehmerbeschwerden aber auch von Anfragen von Anbieterseite stellte sich im Berichtszeitraum mehrfach die Frage, in welchem Maße Kommunikations- und Sicherheitsmaßnahmen in Betrieben noch zulässig sind, wenn diese über den angegebenen Zweck hinaus auch zur unmittelbaren Überwachung und Leistungskontrolle von Mitarbeiter genutzt werden bzw. in dieser Weise objektiv wirken könnten oder subjektiv so empfunden werden.

Je nach individueller Fallgestaltung ging es um Kommunikationseinrichtungen wie Mikrofone und Kameras, die der Verständigung zwischen Mitwirkenden an Produktionsprozessen dienen sollten, aber auch um Einrichtungen, die der Sicherung spezieller Räume zur Lagerung wertvoller Gegenstände, oder auch der Überwachung von allgemeinen Verkehrsflächen aus anderen Gründen zu dienen bestimmt sein sollten.

In jedem Fall waren zunächst die individuellen Gegebenheiten, die Lage der technischen Einrichtungen in den jeweiligen Räumlichkeiten und die Gefährdungslage zu ermitteln, um sodann eine Abwägung der berührten Einzelinteressen vornehmen zu können. In einem Fall erschien es sogar im Hinblick auf die nachhaltig vorgetragenen Einwendungen notwendig, trotz vorgelegter Planunterlagen und weiterer Erläuterungen eine auswärtige Ortsbesichtigung durchzuführen, um die Sachlage hinreichend aufklären zu können.

In jedem Fall kommt es darauf an, die betrieblichen Belange wie auch die berührten Interessen der betroffenen Mitarbeiter genau zu ermitteln, um eine hinreichende Grundlage für die vorzunehmende Abwägung erarbeiten zu können. Kann der Betrieb die Erforderlichkeit der Einrichtungen glaubhaft machen und werden die Mitarbeiter hinreichend über deren Einsatz informiert und die Einsatzzeiten ggf. auch kenntlich gemacht oder sind gar technisch nachprüfbar, können Einrichtungen datenschutzrechtlich durchaus zulässig sein, auch wenn keine hinreichenden Anhaltspunkte für Straftaten vorliegen, deren Aufdeckung den Einsatz der Einrichtungen erforderlich erscheinen lassen und so rechtfertigen würde.

5.4 Datenpannen

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

Nachdem bereits kurz vor Beginn des Berichtszeitraumes eine Datenpanne gemeldet worden war, kamen im Berichtszeitraum zwei weiteren Meldungen hinzu, was die stetig wachsende Bedeutung der häufig thematisierten Fragen der Datensi-

cherheit unterstreicht.

Der Fall des Jahres 2011 betraf wie bereits berichtet einen Hackerangriff; da sich dieser aber nur auf die Daten der Teilnehmer an einem unentgeltlichen Gewinnspiel richtete, waren zwar personenbezogene Daten der Mitspieler, jedoch keine sensiblen Daten im Sinne des § 3 Abs. 9 BDSG oder spezielle personenbezogene Daten nach § 42a Abs. 1 Nr. 1-4 BDSG betroffen, so dass der Fall als weniger gravierend eingestuft werden konnte.

Im Berichtszeitraum trat nunmehr jedoch eine Datenpanne auf, von der neben Name, Anschrift und Geburtsdaten auch Bank- und Kreditkartendaten betroffen waren. Derartige Daten lösen die besonderen Informationsplichten des § 15a TMG bzw. § 42a BDSG aus.

Konkret wurden Kundendaten in einer nicht unerheblichen Größenordnung von einer dritten Person abgezogen und mehrstufig weitergereicht, so dass die betroffenen Kunden durch Anrufe in unterschiedlicher Weise belästigt wurden. Die Anrufer meldeten sich teils als beauftragte Vermittler von Zusatzgeschäften, Veranstalter von Gewinnspielen aber auch als beauftragte Inkassostelle der vorgenannten oder beliebiger anderer Dritter, so dass durchaus die in § 42a S. 1 BDSG genannten schwerwiegenden Beeinträchtigungen drohten.

Der Beauftragte für den Datenschutz wurde pflichtgemäß zeitnah über die Datenpanne informiert. Der Anbieter hat zudem umgehend fachkundige Hilfe von dritter Seite eingeholt, eingehende Nachforschungen angestellt und auch das Cyber Allianz Zentrum Bayern sowie die Strafverfolgungsbehörden eingeschaltet, so dass umfangreiche für die Zukunft wirkende präventive wie auch in die Vergangenheit gerichtete repressive Maßnahmen ergriffen wurden, die wohl letztlich auch entsprechende Ergebnisse erbrachten. Die maßgeblichen Verfahren dauern noch an.

Hinzu kamen unsere eigenen Prüfungen, die von großer Offenheit seitens des betroffenen Anbieters geprägt waren. Diese erstreckten sich insbesondere auf die Frage, woher das Datenleck rührte, wie sich der unberechtigte Zugriff ereignete, auf welchen Zeitraum er entfiel, welches Ausmaß er annahm und ob den erforderlichen Benachrichtigungspflichten des Anbieters hinsichtlich der betroffenen Kunden genügt wurde. Dies Prüfungen gingen deutlich über den Berichtszeitraum hinaus.

Daneben erreichte uns natürlich auch eine erhebliche Anzahl von Datenschutzbeschwerden, die den Vorfall betrafen. Die Beschwerdeführer fühlten sich verständlicherweise in erheblichem Maße gerade im Hinblick auf die betroffenen Bank- und Kreditkartendaten verunsichert. Die uns möglichen Auskünfte und Rückmeldungen, dass wir wie auch die Strafverfolgungsbehörden bereits informiert und tätig seien und es erste Ermittlungsergebnisse gebe, konnte etwas zur Beruhigung beitragen. Das in § 42a BDSG vorgesehene Prozedere hat sich in diesem Rahmen als

durchaus sinnvoll erwiesen.

Unmittelbar im Monat nach der Meldung der oben genannten Datenpanne wurden wir über ein wohl tatsächliches weiteres Datenleck eines anderen Anbieters informiert, auf das der betroffene Anbieter durch einen anonymen Anrufer hingewiesen wurde, der nach den uns vorliegenden Informationen offenbar keine Gegenleistung forderte oder erwartete.

Gleichwohl waren wir wie in § 42a BDSG vorgesehen umgehend informiert worden. Da sich aber in der Folgezeit keine Hinweise auf Datenverluste einstellten, und auch keine diesbezüglichen Beschwerden bei uns bzw. dem Anbieter eingingen, ist davon auszugehen, dass tatsächlich keine Daten an Dritte weitergeleitet wurden bzw. zur Kenntnis gelangt sind, es sich damit um keinen Fall des § 42a BDSG im eigentlichen Sinne handelte, und der Fall offenbar glücklicherweise auch keine unliebsamen Auswirkungen hatte.

5.5 Rundschreiben an die Datenschutzbeauftragten der Anbieter

Da die datenschutzrechtlichen Fragestellungen insgesamt umfangreicher und brisanter wurden, erschien es angezeigt, die Anbieter über die aktuellen Gesetzesentwickelungen zu informieren. In einem umfangreichen Schreiben wurden die Anbieter über die Folgen der Harmonisierung von Rundfunk und Telemedien durch den 9. Rundfunkänderungsstaatsvertrag, die wesentlichen Änderungen der BDSG-Novellen und aktuelle Themen wie "Social-Plugins", "Facebook-Like-Button" und die datenschutzkonforme Verwendung von Google-Analytics informiert. Da mit diesem Schreiben zugleich der aktuelle Stand des Einsatzes von betrieblichen Datenschutzbeauftragten abgefragt wurde, waren in diesem Schreiben auch die Voraussetzungen der Bestellung eines Betrieblichen Datenschutzbeauftragten erklärt.

Das Informationsschreiben führte zu zahlreichen anbieterseitigen Rückfragen und zu einem regen Austausch über die angesprochenen Fragen, der bis heute andauert. Die eingeschlagene Vorgehensweise hat sich aus unserer Sicht durchaus bewährt und wird zu gegebener Zeit fortgeführt werden.

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 der 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, 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 mit Fragen der Rechtsfortbildung und seit dem Ende 2012 verstärkt mit den Inhalten, Vorteilen und Schwächen und Folgewirkungen der EU-Datenschutz-Grundverordnung befassen.

Neben dem Brennpunkt "Datenschutzgrundverordnung" wurden z.B. Veranstaltungen zu Fragen handhabbarer Messverfahren, Metriken und Marity Models für die Bestimmung des Datenschutzniveaus im Unternehmen, zum Thema BYOD (Birng Your Own Device) besucht.

Besonderes Augenmerk widmete der Beauftragte für den Datenschutz gemeinsam mit dem Leiter IT dem Thema "IT-Recht und Sicherheit – Aspekte eines Sicherheitskonzepts" im Rahmen einer mehrtätigen Fortbildung. Die Veranstaltung diente dazu im Hinblick auf Gefahren zu sensibiliseiren, die durch Angriffe, Sicherheitslücken von Anwendungen und Diensten und durch E-Mailkorrespondenz drohen. Es wurden Optionen für organisatorische Ansätze für mehr IT-Sicherheit (IT-Sicherheits- und Datenschutzbeauftragter, IT-Sicherheitsrichtlinie, IT-Sicherheitskonzepte, BSI-Grundschutz-Qualifizierung, Betriebs- und Geheimhaltungsvereinbarungen) sowie die technischen Möglichkeiten und deren rechtliche Grenzen aufgezeigt.

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

Im Dezember 2013 fand ein Treffen im Bayerischen Landesamt für Datenschutzaufsicht in Ansbach zum Thema Smart-TV statt. Das Landesamt stellte erstmals seine Untersuchungen zu diesem Thema und insbesondere der Frage, welche Datenflüsse auf internetfähigen Fernsehern stattfinden, vor und wie diese Datenflüsse sichtbar gemacht werden können. Der Präsident des Landesamtes machte in einem Interview mit

zahlreichen Pressevertretern deutlich, dass man anhand solcher Datensammlungen nachvollziehen könne, wer wann welche Sendung schaue; auch könne man Profile der Zuschauer zu deren politischen Einstellung erstellen[107].

Während das Thema SmartTV vor allem die Hersteller von Fernsehgeräten und damit die staatliche Aufsicht über den nicht-öffentlichen Bereich betrifft, werden bei dem damit verwandten Thema Hbb-TV die Rundfunkveranstalter selbst und damit die rundfunkrechtlichen Aufsichtsinstitutionen angesprochen. Dies hat in der Folgezeit zu zahlreichen Aktivitäten von Seiten der Anbieter, der Datenschutzaufsicht wie auch der Landesmedienanstalten geführt, die die besondere Brisanz des Themas verdeutlichen, andererseits aber auch den Blick auf keineswegs neue aber dennoch zumeist unlösgelöste Fragen insbesondere im Hinblick auf Zuständigkeiten und die Wahrung der Staatsferne im Rundfunk lenken sollten, da das Thema HbbTV die seit langem beschworene Konvergenz nun praktisch unmittelbar eintreten lässt.

[107] Vgl. Lokales Tagesblatt Ansbach FLZ AN 3.12.13.

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, entwickelt sich gerade aus diesem Bereich und insbesondere aus 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. Neben den Zukunftsthemen Plattformen für Rundfunk- und Telemedien und ggf. auch Suchmaschinen zeigt sich dies in den Entwicklungen, die unter den Stichworten SmartTV und HbbTV diskutiert werden und nach dem Ende des Berichtszeitraumes anknüpfend an die unter 6. geschilderten Erkenntnisse des Landesamtes eine lebhafte Diskussion zu Fragen des Datenschutzes (insbesondere in Bezug auf den Fernseher im Wohnzimmer) hervorgebracht haben.