

Bayerische Landeszentrale für neue Medien

Neunter Tätigkeitsbericht
des Beauftragten für den Datenschutz
bei der Bayerischen Landeszentrale für neue Medien
(Berichtszeitraum: 01.01.2008 bis 31.12.2009)

An den
Vorsitzenden des Medienrats
Herrn Dr. Erich Jooß

Vorsitzenden des Verwaltungsrats
Herrn Manfred Nüssel

Präsidenten der
Bayerischen Landeszentrale
für neue Medien
Herrn Professor
Dr. Wolf-Dieter Ring

im Hause

Ihr Zeichen/Ihre Nachricht vom

Unser Zeichen

Telefon

Datum

Az.: 3./5

63808-161

09.02.2011

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

Sehr geehrter Herr Dr. Jooß,
sehr geehrter Herr Nüssel,
sehr geehrter Herr Professor Dr. Ring,

in der Anlage übersende ich Ihnen gemäß Art. 20 Abs. 6 Satz 2 des Bayerischen Mediengesetzes den achten Tätigkeitsbericht des Beauftragten für den Datenschutz bei der Bayerischen Landeszentrale für neue Medien.

Mit freundlichen Grüßen

Andreas Gummer
Beauftragter für den Datenschutz

INHALTSVERZEICHNIS

1. Vorbemerkung
2. Entwicklung des Datenschutzrechts
 - 2.1. Europäisches Recht
 - 2.1.1. Der Vertrag von Lissabon
 - 2.1.2. Urteil des EuGH zur Vorratsdatenspeicherung
 - 2.1.3. Urteil des EuGH zur Unabhängigkeit des Datenschutzbeauftragten
 - 2.1.4. Richtlinie 2009/136/EG
 - 2.2. Bundesrecht
 - 2.2.1. Bundesdatenschutzgesetz (BDSG)
 - 2.2.1.1. Novelle I - Gesetz vom 29. Juli 2009
 - 2.2.1.2. Novelle II - Gesetz vom 14. August 2009
 - 2.2.1.3. Novelle III - Gesetz vom 29. Juli 2009
 - 2.2.2. Telekommunikationsgesetz (TKG)
 - 2.2.3. Telemediengesetz (TMG)
 - 2.2.4. Allgemeines Gleichbehandlungsgesetz (AGG)
 - 2.2.5. Informationsfreiheitsgesetz des Bundes (IFG)
 - 2.2.6. Gesetz über das Verfahren des elektronischen Entgeltnachweises (sog. ELENA-Verfahrensgesetz) vom 28. März 2009
 - 2.2.7. Novellierung des „Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (sog. BKA-Gesetz)
 - 2.2.8. Urteil des BVerfG zur Online-Durchsuchung

- 2.3. Bayerisches Landesrecht
 - 2.3.1. Art. 21 a BayDSG
 - 2.3.2. Rundstaatsvertrag (RStV)
 - 2.3.3. Bayerisches Mediengesetz (BayMG)
- 3. Funktion des Beauftragten für den Datenschutz
- 4. Datenschutz in der Landeszentrale
 - 4.1. Allgemeines
 - 4.1.1. Datenschutzrechtliche Freigabe automatisierter Verfahren nach Art. 26 BayDSG
 - 4.1.2. Verzeichnisse nach Art. 27 BayDSG
 - 4.2. Verwaltungsgebäude der Landeszentrale
 - 4.3. Mitarbeiterschulung
- 5. Datenschutz bei den Anbietern und Tochtergesellschaften der Landeszentrale

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 neunte Tätigkeitsbericht seit Inkrafttreten des BayMG am 01.12.1992 und bezieht sich auf die Jahre 2008 und 2009.

Der Schwerpunkt meiner Tätigkeit lag im Berichtszeitraum neben der Beratung von Landeszentrale und Anbietern hinsichtlich der Anforderungen des Datenschutzrechts und der sich für den betrieblichen Ablauf daraus ergebenden Folgerungen vor allem auch in der anlassbezogenen Kontrolle der Einhaltung und Umsetzung datenschutzrechtlicher Vorgaben aufgrund wie auch unabhängig von eingehenden Beschwerden.

Förmliche Beanstandungen musste ich im Berichtszeitraum nicht aussprechen.

2. Entwicklung des Datenschutzrechts

2.1. Europäisches Recht

Das nationale Datenschutzrecht ist zunehmend durch Vorgaben der Europäischen Union geprägt. Den grundlegenden Rahmen gibt die EU-Datenschutzrichtlinie¹ vor, die die Harmonisierung der sich aus dem Datenschutz ergebenden Anforderungen im Hinblick auf einen einheitlichen Wirtschaftsrahmen als Ziel verfolgt.

2.1.1. Der Vertrag von Lissabon

Der Vertrag von Lissabon, der am 13. Dezember 2007 von den europäischen Staats- und Regierungschefs unterzeichnet worden ist, bringt nach dem Inkrafttreten am 1. Dezember 2009 maßgebliche Änderungen für den Datenschutz. Durch den Vertrag von Lissabon werden die bislang geltenden Gemeinschaftsverträge grundlegend umgestaltet. Eine entscheidende Neuerung ist die Aufhebung der Säulenstruktur² und die Einbindung der Charta der Grundrechte in das europäische Primärrecht. Für den datenschutzrechtlichen Bereich ergeben sich daraus folgende Änderungen:

¹ Richtlinie 95/46/EG, ABl. EG v. 23.11.1995, Nr.L 281/31. Im Telekommunikationsbereich wird die Datenschutzrichtlinie durch die im Jahr 2002 erlassene Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) ergänzt.

² 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).

- gem. Art. 16 Abs. 2 AEUV³ verpflichten sich die europäischen Gesetzgebungsorgane zum Erlass von Datenschutzvorschriften; die Einhaltung dieser Vorschriften soll von unabhängigen Behörden überwacht werden. Diese Verpflichtung gilt nicht nur für die Verarbeitung personenbezogener Daten durch europäische Institutionen, sondern nunmehr auch für die Verarbeitung von Daten durch die Mitgliedsstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Unionsrecht fallen.
- der Vertrag von Lissabon führt zu einem Wegfall der bisherigen Säulenstruktur. Der bisher der dritten Säule zugehörige Bereich der zwischenstaatlichen polizeilichen- und justiziellen Zusammenarbeit wird damit „vergemeinschaftet“ und unterliegt folglich grundsätzlich auch dem Geltungsbereich des Art. 16 AEUV. Inwieweit die EU- Datenschutzrichtlinie (95/46/EG), die bislang gerade nicht für den Sicherheitsbereich galt, nunmehr hier Anwendung findet, ist noch offen.
- am 27. November 2008 hat der Rat der EU-Innen- und Justizminister einen Rahmenbeschluss über den Datenschutz in der dritten Säule verabschiedet.⁴ Es erscheint jedoch zweifelhaft, ob dieser den Anforderungen des Art. 16 AEUV entsprechen wird. Problematisch ist insbesondere, dass der Rahmenbeschluss sich nur auf die grenzüberschreitende Kommunikation und nicht auf die Datenverarbeitung in den Mitgliedsstaaten selbst bezieht, obwohl die übermittelten Daten im Empfängerland mit den dort erhobenen Daten zusammengeführt werden. Als unbefriedigend wird der Beschluss auch hinsichtlich des Rechtes des Betroffenen auf Auskunft empfunden, weil die konkrete Ausgestaltung den Mitgliedsstaaten überlassen wurde.
- die wohl wichtigste Änderung ist jedoch die Bezugnahme auf die Charta der Grundrechte im Vertrag von Lissabon. In Art. 8 der Grundrechtecharta ist ein Grundrecht auf Datenschutz normiert, das zum ersten Mal auf europäischer Ebene rechtsverbindlich ist. Noch ist nicht abzusehen, welche Auswirkungen die unmittelbare Geltung der EU-Grundrechte auf den Datenschutz auf nationaler Ebene haben wird. Das bewährte Grundrecht auf informationelle Selbstbestimmung darf durch europäische Regelungen zwar ergänzt, aber nicht verdrängt werden, da die europäischen Grundrechte noch kein vergleichbares Schutzniveau gewährleisten.⁵

³ Vertrag über die Arbeitsweise der Europäischen Union.

⁴ ABl. EU 2008/L 350/60.

⁵ Vgl. *Ronellenfisch*, Der Vorrang des Grundrechts auf informationelle Selbstbestimmung vor dem AEUV, DuD, 2009, S. 451 ff.

2.1.2. Urteil des EuGH zur Vorratsdatenspeicherung

Mit seiner Klage hatte Irland beantragt, die Richtlinie 2006/24/EG⁶ des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG für nichtig zu erklären, da sie nicht auf einer geeigneten Rechtsgrundlage erlassen wurde. Die irische Regierung machte geltend, die Vorratsdatenspeicherung diene der Bekämpfung schwerer Verbrechen und hätte deshalb als EU-Rahmenbeschluss im Bereich der Polizei- und Justizzusammenarbeit verabschiedet werden müssen. Die Slowakei hat sich der irischen Klage angeschlossen, argumentiert aber, die Vorratsdatenspeicherung führe zu einem erheblichen Eingriff in das Recht Einzelner auf Achtung des Privatlebens nach Art. 8 EMRK.

Am 10. Februar 2009 hat der EuGH nunmehr in einem Urteil⁷ entschieden, dass die Richtlinie (2006/24/EG) auf der Grundlage des EG-Vertrages, insbesondere Art. 95 EG, wirksam erlassen wurde. Der EuGH stellte hierbei klar, dass die Entscheidung keinerlei Aussage zu einer möglichen Verletzung der Grundrechte durch die Richtlinie in materieller Hinsicht trifft, sondern sich lediglich auf die richtige Wahl der Rechtsgrundlage bezieht.

Nach Art. 95 Abs. 1 EG erlässt der Rat die Maßnahmen zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten, die die Errichtung und das Funktionieren des Binnenmarkts zum Gegenstand haben. Der Gemeinschaftsgesetzgeber kann Art. 95 EG insbesondere im Fall von Unterschieden zwischen den nationalen Regelungen heranziehen, wenn diese Unterschiede geeignet sind, die Grundfreiheiten zu beeinträchtigen oder Wettbewerbsverzerrungen zu verursachen, und sich auf diese Weise unmittelbar auf das Funktionieren des Binnenmarkts auswirken.

In diesem Zusammenhang weist der Gerichtshof darauf hin, dass mehrere Mitgliedstaaten bereits zuvor Regelungen erlassen hätten, die insbesondere hinsichtlich der Natur der gespeicherten Daten und ihrer Speicherungsfrist erheblich divergierten. Diese Verpflichtungen zur Vorratsdatenspeicherung brächten *erhebliche wirtschaftliche Auswirkungen* für die Dienstanbieter mit sich, da sie grundsätzlich hohe Investitionen und Betriebskosten nach sich zögen. Die bereits bestehenden Unterschiede zwischen den nationalen Maßnahmen könnten sich noch verstärken, sobald weitere Mitgliedsstaaten ebenfalls entsprechende Vorschriften erlassen. Dies wirke sich unmittelbar auf das Funktionieren des Binnenmarkts aus. Daher sei es gerechtfertigt,

⁶ ABl. EG v. 15.03.2006, Nr. L 105/54.

⁷ Urteil des Europäischen Gerichtshofs vom 10. Februar 2009, Az: C-301/06.

dass der Gemeinschaftsgesetzgeber das Ziel, das Funktionieren des Binnenmarkts zu schützen, durch den Erlass von Harmonisierungsvorschriften verfolgte.⁸

In Deutschland wurde die Richtlinie mit dem „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer versteckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“⁹ umgesetzt. Das Gesetz wurde am 09.11.2007 im Bundestag verabschiedet und am 26.12.2007 vom Bundespräsidenten unterzeichnet. Es trat am 01.01.2008 in Kraft. Das Bundesverfassungsgericht hat das deutsche Gesetz zur Vorratsdatenspeicherung, mit dem die EU- Richtlinie umgesetzt wurde, auf die Vereinbarkeit mit dem deutschen Grundgesetz geprüft und verworfen.¹⁰

2.1.3. Urteil des EuGH zur Unabhängigkeit des Datenschutzbeauftragten

Die Europäische Kommission hatte am 05.07.2005 ein Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland eingeleitet. Mit der Klage verfolgte die Europäische Kommission die Absicht, die Bundesrepublik Deutschland zur Einführung eines im Sinne der EU- Datenschutzrichtlinie¹¹ unabhängigen Datenschutzbeauftragten zu bewegen.

Die Kommission monierte zuvor, dass die Datenschutzaufsicht über die Privatwirtschaft, so wie sie derzeit organisiert sei, nicht über die von der EU- Datenschutzrichtlinie geforderte „**völlige Unabhängigkeit**“ verfüge. Art. 28 Abs. 1 dieser Richtlinie sieht die Einrichtung von öffentlichen Kontrollstellen in den einzelnen Mitgliedsstaaten vor, die die Anwendung der zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in völliger Unabhängigkeit überwachen. Die derzeitige Organisation der Datenschutzaufsicht für den nicht-öffentlichen Bereich sei mit dieser Vorschrift nicht vereinbar, da die bestehenden unterschiedlichen Organisationsformen der Kontrollstellen in den Bundesländern insbesondere im Hinblick auf die verschiedenen Formen staatlicher Aufsicht über diese Stellen nicht den Anforderun-

⁸ Diese Begründung erscheint vor allem deshalb diskussionswürdig, weil die Richtlinie keineswegs nur Speicherungspflichten harmonisiert, sondern solche Verpflichtungen auch für die Länder verbindlich einführt, in denen es bis dahin keine derartige Verpflichtung gab, und zudem auch berechtigte Zweifel bestanden, ob alle nationalen Gesetzgeber eine solche Verpflichtung einführen könnten, geschweige denn würden. Ebenso erscheint zweifelhaft, ob eine solche Verpflichtung wirklich für das Funktionieren des Binnenmarktes erforderlich ist. Die Richtlinie hat tiefer gehende Auswirkungen auf den realen Datenschutz der Gemeinschaftsbürger gegenüber den Sicherheitsbehörden als jede andere europäische Regelung, weil sie die Unternehmen in den Mitgliedstaaten zur Erzeugung und dauerhaften Speicherung riesiger Datensammlungen verpflichtet, die nach Maßgabe des nationalen Rechts einem weitgehenden behördlichen Zugriff für Zwecke der Sicherheit und der Strafverfolgung unterliegen.

⁹ BGBl I 2008, S. 70.

¹⁰ Urteil des BVerfG vom 02. März 2010, BVerfGE 125, 260 ff, vgl. unten 2.2.2.

¹¹ Richtlinie 95/46/EG, ABl. EG v. 23.11.1995, Nr. L 281, S. 31

gen der Richtlinie im Hinblick auf die Unabhängigkeit dieser Kontrollstellen entsprechen.

Im Gegensatz dazu vertrat die Bundesrepublik Deutschland in diesem Verfahren die Auffassung¹², dass die Richtlinie insoweit nur eine relative Unabhängigkeit der Aufsichtsbehörden von den zu kontrollierenden Stellen im privaten Bereich im Auge habe und im Übrigen die Verfassungsstruktur und die Organisation der Staatsgewalt in dem jeweiligen Mitgliedsstaat unberührt lasse.

Inzwischen liegt ein Urteil des EuGH vom 09. März 2010¹³ vor, in dem der Gerichtshof über das Vertragsverletzungsverfahren entschieden hat. Der EuGH hat entschieden, dass die Bundesrepublik Deutschland gegen ihre Verpflichtungen aus Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr verstoßen hat, indem sie die für die Überwachung der Verarbeitung personenbezogener Daten durch nicht-öffentliche Stellen und öffentlich-rechtliche Wettbewerbsunternehmen zuständigen Kontrollstellen in den Bundesländern staatlicher Aufsicht unterstellt und damit das Erfordernis, dass diese Stellen ihre Aufgaben „in völliger Unabhängigkeit“ wahrnehmen, falsch umgesetzt hat.

In Bezug auf öffentliche Stellen bezeichne der Begriff „Unabhängigkeit“ nach Auffassung des EuGH in der Regel eine Stellung, in der gewährleistet sei, dass die betreffende Stelle völlig frei von Weisungen und Druck handeln könne. Entgegen dem Standpunkt der Bundesrepublik Deutschland deute nichts darauf hin, dass das Unabhängigkeitserfordernis allein das Verhältnis zwischen den Kontrollstellen und den ihrer Kontrolle unterstellten Einrichtungen betreffe. Vielmehr werde der Begriff „Unabhängigkeit“ noch durch das Adjektiv „völlig“ verstärkt, was eine Entscheidungsgewalt impliziere, die jeglicher Einflussnahme von außerhalb der Kontrollstelle, sei es unmittelbar oder mittelbar, entzogen sei.¹⁴

Für den Bereich der Landeszentrale bestehen derartige Zweifel an der Unabhängigkeit des Beauftragten für den Datenschutz nicht; dieser ist nach Art. 20 Abs. 3 S. 6 BayMG in der Ausübung seines Amtes, auch bei der Aufsicht über die Landeszentrale selbst, unabhängig und nur dem Gesetz unterworfen.¹⁵ Da auch die gelebte Praxis bei der Landeszentrale diesen Vorga-

¹² Vgl. die Mitteilung über die Klageeinreichung im Amtsblatt der Europäischen Union vom 09.02.2008 zur Rechtssache C-518/07.

¹³ Urteil des EuGH vom 09. März 2010, C- 518/07.

¹⁴ Da das Urteil erst am 09.03.2010 und damit außerhalb des Berichtszeitraumes ergangen ist, beschränkt sich der vorliegende Tätigkeitsbericht auf die angegebenen wesentlichsten Kernaussagen.

¹⁵ Vgl. dazu unten die Ausführungen zur Funktion des Beauftragten für den Datenschutz unter 3.

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

2.1.4. Richtlinie 2009/136/EG¹⁶

Am 25. November 2009 haben das Europäische Parlament und der Rat der Europäischen Union Änderungen der Datenschutzrichtlinie für elektronische Kommunikation¹⁷ beschlossen. Die Neufassung der Richtlinie ist am 19. Dezember 2009 in Kraft getreten.

Gemäß der RL 2009/136/EG wird Art. 4 der RL 2002/58/EG um eine Informationspflicht im Falle einer Verletzung des Schutzes personenbezogener Daten ergänzt. Nach Art. 4 Abs. 3 S. 1 n. F. hat der Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste im Falle einer Verletzung des Schutzes personenbezogener Daten unverzüglich die zuständige nationale Behörde von der betreffenden Verletzung zu benachrichtigen. Nach Art. 4 Abs. 3 S. 2 n. F. hat er darüber hinaus auch die Teilnehmer bzw. betroffenen Personen unverzüglich von der Verletzung zu benachrichtigen, wenn anzunehmen ist, dass diese durch die Verletzung des Schutzes personenbezogener Daten in ihrer Privatsphäre beeinträchtigt werden.

Die hier vorgesehene Informationspflicht ist weitergehend als die Informationspflicht, welche beispielsweise in § 42 a BDSG, § 15 a TMG und § 93 Abs. 3 TKG vorgesehen ist. Die Informationspflicht greift danach nicht nur bei einer unrechtmäßigen Übermittlung von Daten, sondern darüber hinaus auch bei jeder Art von Sicherheitsverletzung, die auf unbeabsichtigte oder unrechtmäßige Weise zur Vernichtung, zum Verlust oder zur Veränderung der Daten führt. Das Qualifikationsmerkmal der „schwerwiegenden Beeinträchtigungen“ wird in der Richtlinie nicht erwähnt. Die Dienstanbieter werden zudem verpflichtet, ein Verzeichnis der Verletzungen des Schutzes personenbezogener Daten zu führen. Die Richtlinie muss bis zum 25.05.2011 in nationales Recht umgesetzt werden; hierbei wird die Anpassung der bisherigen Informationspflichtenregelungen im deutschen Datenschutzrecht erforderlich werden.¹⁸

¹⁶ Richtlinie zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 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.

¹⁷ RL 2002/58/EG sog. E-Privacy-Richtlinie.

¹⁸ Vgl. Moos, Die Entwicklung des Datenschutzrechts im Jahr 2009, K&R 3/2010, S. 170.

2.2 Bundesrecht

2.2.1. Bundesdatenschutzgesetz (BDSG)

Im Jahr 2009 hat der Bundestag zahlreiche gravierende Änderungen des Bundesdatenschutzgesetzes beschlossen, die in den sog. Novellen I, II und III umgesetzt wurden.

2.2.1.1 Novelle I - Gesetz vom 29. Juli 2009¹⁹

Die Schwerpunkte dieser Gesetzesnovelle lagen auf Auskunftfeien und dem sog. Scoring. Das Ziel war es hier, die Tätigkeit von Auskunftfeien und ihren Vertragspartnern transparenter zu machen, indem Informations- und Auskunftsrechte von Betroffenen gestärkt werden. Zudem enthält das Gesetz spezifische Erlaubnistatbestände und Regelungen für sog. Scoringverfahren.²⁰ Im Zuge dessen wurden zwei völlig neue Tatbestände geschaffen:

- Gem. **§ 28 a BDSG** sind Datenübermittlungen an Auskunftfeien nur dann zulässig, wenn eine geschuldete Leistung trotz Fälligkeit nicht erbracht worden ist, die Übermittlung zur Wahrung berechtigter Interessen der verantwortlichen Stelle oder eines Dritten erforderlich ist und einer der in § 28 a Abs. 1 Nr. 1-5 BDSG abschließend aufgeführten Fälle vorliegt.
- Gem. **§ 28 b BDSG** dürfen Scorewerte zur Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses nur verwendet werden, wenn ein wissenschaftlich anerkanntes mathematisch- statistisches Verfahren verwendet wird, nur Daten genutzt werden, die ohnehin für eigene Zwecke genutzt bzw. an einen Kunden übermittelt werden dürfen, nicht ausschließlich Adressdaten genutzt werden und vor der Nutzung von Adressdaten Betroffene über das beabsichtigte Scoring informiert wurden.

Die oben genannten Änderungen traten am 1. April 2010 in Kraft.

¹⁹ Gesetz zur Änderung des Bundesdatenschutzgesetzes vom 29. Juli 2009, BGBl. I 2009, S. 2254.

²⁰ Mathematisch-statistische Verfahren zur Berechnung der Wahrscheinlichkeit eines bestimmten Verhaltens, insbesondere zur Kreditwürdigkeit einer Person.

2.2.1.2. Novelle II - Gesetz vom 14. August 2009²¹

Mit der Novelle II wurden insgesamt 18 Paragraphen des BDSG geändert.

- In der Neufassung des **§ 3 a BDSG** wird nun für alle Erhebungen, Verarbeitungen und Nutzungen die Pflicht zur Datensparsamkeit und Anonymisierung festgelegt. Die Zielvorgabe des Grundsatzes erstreckt sich nunmehr generell auf die Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Es sollen grundsätzlich so wenig personenbezogene Daten wie möglich erhoben, verarbeitet oder genutzt werden. Wenn darüber hinaus die Möglichkeit zur Anonymisierung oder Pseudonymisierung besteht, so ist diese zu nutzen, soweit dadurch kein unverhältnismäßiger Aufwand entsteht und dies nach dem Verwendungszweck möglich ist.
- Die in **§ 4 f Abs. 1 BDSG** vorgesehenen Voraussetzungen, nach denen Unternehmen zur Bestellung eines betrieblichen Datenschutzbeauftragten verpflichtet sind, wurden erweitert. Diese Verpflichtungen bestehen
 - generell, wenn die verantwortliche Stelle *mehr als neun Arbeitnehmer* mit automatisierter Datenerhebung, -verarbeitung oder -nutzung oder
 - *mindestens zwanzig Arbeitnehmer* mit nichtautomatisierter Datenerhebung, -verarbeitung oder -nutzung beschäftigt (§ 4 f Abs. 1 S. 3, S. 4 BDSG).
 - *unabhängig* von der Zahl der Beschäftigten, wenn die verantwortliche Stelle automatisierte Datenverarbeitungsvorgänge vornimmt, die eine Vorabkontrolle verlangen (z.B. Scoringverfahren, soweit sie selbst Entscheidungscharakter haben) gem. § 4 f Abs. 1 S. 6 BDSG.
 - *unabhängig* von der Zahl der Beschäftigten, neuerdings auch wenn die verantwortliche Stelle personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung oder der anonymisierten Übermittlung erhebt, verarbeitet oder nutzt (Beispiele: Adressverlage, Markt- und Meinungsforschungsinstitut) gem. § 4 f Abs. 1 S. 6 BDSG.

²¹ Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 14. August 2009, BGBl. I 2009, S. 2814.

Die Position des betrieblichen Datenschutzbeauftragten wurde durch die Verbesserung des Kündigungsschutzes gestärkt. Gem. § 4 f Abs. 3 S. 5 BDSG ist nun zweifelsfrei gesetzlich klargestellt, dass der betriebliche Datenschutzbeauftragte grundsätzlich nicht ordentlich kündbar ist. Einem betrieblichen Datenschutzbeauftragten kann nur bei Vorliegen eines wichtigen Grundes i.S.d. § 626 BGB gekündigt werden. Der Kündigungsschutz wirkt auch nach der Abberufung des Datenschutzbeauftragten für eine Dauer von einem Jahr nach. Darüber hinaus hat die verantwortliche Stelle dem Datenschutzbeauftragten gem. § 4 f Abs. 3 S. 7 BDSG die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und deren Kosten zu übernehmen. Damit ist das Recht des Datenschutzbeauftragten auf Fort- und Weiterbildung explizit geregelt.

- Die Anforderungen an die Auftragsdatenverarbeitung in **§ 11 BDSG** wurden verschärft. Eine Auftragsdatenverarbeitung liegt dann vor, wenn personenbezogene Daten im Auftrag eines Auftraggebers durch eine andere Stelle erhoben, verarbeitet oder genutzt werden (Outsourcing). In diesem Fall verbleibt die Verantwortung für die ordnungsgemäße Datenverarbeitung beim Auftraggeber.

In **§ 11 Abs. 2 BDSG** werden die Bedingungen der Auftragsdatenverarbeitung aufgezählt. Neu ist, dass der Mindestgehalt des der Auftragsverwaltung zugrundeliegenden Vertrages nun gesetzlich detailliert vorgegeben wird. Dazu gehört u.a:

- Gegenstand und Dauer des Auftrags,
- Umfang, Art und Zweck der Datenverwendung, Art der Daten und Kreis der Betroffenen,
- nach § 9 BDSG zu treffende technische und organisatorische Maßnahmen,
- Kontrollpflichten des Auftragnehmers,
- Kontrollrechte des Auftraggebers und Umfang der Weisungsbefugnisse,
- mitzuteilende Verstöße des Auftragnehmers gegen datenschutzrechtliche Vorschriften.

Insgesamt ist der Katalog der Mindestinhalte von Auftragsdatenverarbeitungsverträgen auf 10 Regelungsgegenstände ausgedehnt worden, welche in § 11 Abs. 2 BDSG aufgezählt werden.

Der Auftraggeber hat sich dabei erstmals *vor* Beginn der Datenverarbeitung und sodann *regelmäßig* von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen, was aus Gründen der Nachweisbarkeit zu *dokumentieren* ist. Entscheidend ist hierbei also, dass eine erweiterte Kontrolle und Dokumentation sichergestellt werden muss und diese Kontrolle unbedingt *vor* Beginn der Datenverarbeitung erfolgen muss. Gesetzlich nicht geregelt bleibt dabei, welche konkreten Maßnahmen in welchen Intervallen ergriffen werden müssen. Dies ist eine Frage des konkreten Einzelfalls.

Alte Verträge müssen bezüglich dieser formalen Bedingungen nunmehr unbedingt überarbeitet werden. Dies gilt auch für die Verträge, die vor dem 01. September 2009 begründet wurden. Es wurden keine Übergangsfristen oder Ausnahmeregelungen vorgesehen.

- Einer der Kernpunkte der Neuregelungen im BDSG ist die erhebliche Beschränkung der Verwendung personenbezogener Daten für die Zwecke des Adresshandels oder der Werbung, wobei sich die Neuregelung durch ein reichhaltiges Regel- und Ausnahmegewirr auszeichnet.

- Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung für ***eigene Geschäftszwecke*** ist in § 28 Abs. 1 BDSG geregelt. Neu gefasst wurde § 28 Abs. 1 S. 1 Nr. 1 BDSG, wonach die Datenverwendung für eigene Geschäftszwecke zulässig ist, wenn es für die *Be-gründung, Durchführung* oder *Beendigung* eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen *erforderlich* ist.

- Die Verarbeitung und Nutzung personenbezogener Daten für ***Zwecke des Adresshandels oder der Werbung*** sind weiterhin zulässig, wenn der Betroffene *schriftlich eingewilligt* hat (§ 28 Abs. 3 S. 1 BDSG). Damit gilt der Grundsatz, dass die Verarbeitung und Nutzung von personenbezogenen Daten für Zwecke des Adresshandels oder der Werbung einer Einwilligung bedarf.

Bezüglich der Form der Einwilligung gilt: Liegt eine *schriftliche* Einwilligung nicht vor, ist die Nutzung und Verarbeitung personenbezogener Daten nur dann zulässig, wenn eine Einwilligung unter Wahrung der Formerfordernisse nach § 4a Abs. 1

bzw. § 28 Abs. 3 S.1 i.V.m. § 28 Abs. 3a BDSG vorliegt. Wird die Einwilligung also in einer anderen Form als der Schriftform erteilt (z.B. telefonisch), hat die verantwortliche Stelle dem Betroffenen, den Inhalt der Einwilligung *schriftlich zu bestätigen*. Wird die Einwilligung zwar nicht schriftlich, dafür aber *elektronisch* erteilt, muss die verantwortliche Stelle sicherstellen, dass die Einwilligung protokolliert wird und der Betroffene deren Inhalt jederzeit abrufen und die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann.

- *Ohne Einwilligung* zulässig ist gem. § 28 Abs. 3 S. 2 Nr. 1-3 BDSG weiterhin auch die **Verarbeitung oder Nutzung von sog. Listendaten**, jedoch nur, wenn dies erforderlich ist für Zwecke der *Eigenwerbung*, sofern die verantwortliche Stelle die Listendaten beim Betroffenen im Zusammenhang mit der Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnis mit dem Betroffenen bei diesem (selbst generierte Daten) oder aus allgemein zugänglichen Adress-, Rufnummern-, Branchen – oder vergleichbaren Verzeichnissen erhoben hat, oder für *berufsbezogene Werbung* an die berufliche Anschrift (Geschäftswerbung) oder für *Spendenwerbung* zu Gunsten steuerbegünstigter Vereinigungen.

Listendaten in diesem Sinne sind nur Daten, die sich auf die Zugehörigkeit des Betroffenen zu einer Personengruppe, auf Berufs-, Branchen- oder Geschäftsbezeichnung, Namen, Titel, akademischen Grad, Anschrift und das Geburtsjahr beziehen. Telefonnummern oder E-Mail-Adressen gehören weiterhin nicht zu diesen Daten.

Die Übergangsregelung des § 47 BDSG sieht eine Anwendung der alten Regelungen des Listenprivilegs auf vor dem 01. September 2009 zu *Werbezwecken* erhobene oder gespeicherte Daten bis zum **31. August 2012** vor. Trotz dieser Privilegierung für bereits bestehende Datensätze sollten die Unternehmen ihr Datenschutzkonzept jedoch frühzeitig neu ausrichten, um negative Folgen abzuwenden.

- Darüber hinaus ist eine **Übermittlung von Listendaten** für Werbezwecke auch dann ohne Einwilligung des Betroffenen zulässig, wenn die Stelle, die die Daten zum ersten Mal erhoben hat, aus der Werbung eindeutig hervorgeht (§ 28 Abs. 3 S. 4

BDSG). Die *Herkunft der Daten* muss damit eindeutig gekennzeichnet werden! Dabei muss die übermittelnde Stelle die Herkunft der Daten und den Empfänger für eine Dauer von 2 Jahren speichern und dem Betroffenen auf Verlangen Auskunft über die Herkunft der Daten und den Empfänger erteilen (§ 34 Abs. 1a BDSG).

- Im Übrigen dürfen personenbezogene Daten auch für Zwecke der **Werbung für fremde Angebote** genutzt werden, wenn für den Betroffenen bei der Ansprache zum Zwecke der Werbung die für die Nutzung der Daten verantwortliche Stelle eindeutig erkennbar ist. Es ist hierbei davon auszugehen, dass in diesem Fall keine Begrenzung auf Daten nach dem Listenprivileg vorliegt (§ 28 Abs. 3 S. 5 BDSG).
- Gem. § 28 Abs. 3b BDSG dürfen Unternehmen den Vertragsschluss nicht von der Einwilligung in die werbliche Verwendung von Daten abhängig machen (**Koppelungsverbot**). Der Abschluss eines Vertrages darf nicht von der Einwilligung des Betroffenen in die Nutzung seiner Daten abhängig gemacht, wenn dem Betroffenen ein anderer Zugang zu *gleichwertigen* vertraglichen Leistungen ohne die Einwilligung nicht oder in nicht zumutbarer Weise möglich ist. Bei dem auf eine möglichst große verfügbare Meinungsvielfalt ausgerichteten Rundfunkrecht stellt der in diesem Zusammenhang verwendete Begriff der „Gleichwertigkeit“ eine erhebliche Herausforderung dar.²² Die Beibehaltung entsprechender Verknüpfungen in Geschäftsbedingungen führt zu einer Unwirksamkeit der erklärten Einwilligung der Kunden. Diese Grundsatzregel wurde § 28 Abs. 3b Satz 2 BDSG neu eingeführt. Zudem sind Verstöße gegen das Koppelungsverbot als Bußgeldtatbestand ausgestaltet (§ 43 Abs. 2 Nr. 5a BDSG).
- Zu beachten sind darüber hinaus die verschärften Informationspflichten zum **Widerspruchsrecht** des Kunden gem. § 28 Abs. 4 BDSG. Soweit dem Betroffenen in der Vergangenheit das Recht zustand, der Verwendung seiner Daten zu Werbe-

²² Bislang war ein Koppelungsverbot in § 12 Abs. 3 TMG enthalten, der über § 47 Abs. 1 RStV auch für den Rundfunk galt. Das Koppelungsverbot in § 12 Abs. 3 TMG erlaubte eine Kopplung nur, wenn der Zugang zu diesen und nicht nur vergleichbaren Medien in zumutbarer Weise möglich war. Dieser § 12 Abs. 3 TMG ist jedoch aufgrund der Neufassung des TMG vom 01.09.2009 entfallen. § 12 Abs. 3 TMG verweist nunmehr nur noch auf die jeweils geltenden Vorschriften für den Schutz personenbezogener Daten und damit auf § 28 Abs. 3b BDSG.

zwecken insgesamt zu widersprechen, werden Unternehmen nach der neuen Rechtslage verpflichtet, den Betroffenen bereits *bei Vertragsschluss* auf sein Widerspruchsrecht hinzuweisen, was grundsätzlich auch im Rahmen von AGB erfolgen kann.

- Neu hinzugekommen ist nach den letzten Datenschutzskandalen die Regelung des **§ 32 BDSG**. § 32 Abs. 1 BDSG erfasst alle in einem abhängigen Beschäftigungsverhältnis stehenden Personen gem. § 3 Nr. 11 BDSG. Als Rechtsgrundlage für Daten, die in einem Arbeitsverhältnis benötigt werden, dient § 32 Abs. 1 BDSG. § 28 Abs. 1 S.1 Nr. 1 BDSG wird hierdurch im Hinblick auf Beschäftigungsverhältnisse konkretisiert und insoweit verdrängt. Dass dies auch für die Generalklausel des § 28 Abs. 1 S.1 Nr. 2 BDSG gelten soll, liegt bei dem Wortlaut des Gesetzes wie auch der systematischen Stellung der Vorschrift nahe, ist aber strittig. Für den Fall der Zielrichtung der Aufdeckung von Straftaten ist der Wortlaut des § 32 Abs. 1 S. 2 BDSG so eindeutig²³, dass diese Folge bei Anlegung rechtsstaatlicher Grundsätze zwingend erscheint.

Gem. § 32 Abs. 1 S. 1 BDSG dürfen Daten von Beschäftigten erhoben, verarbeitet oder genutzt werden, wenn dies im Rahmen der unterschiedlichen Phasen eines Beschäftigtenverhältnisses erforderlich ist, d.h. bei der *Begründung, Durchführung* oder *Beendigung des Arbeitsverhältnisses*.

Personenbezogene Daten eines Beschäftigten dürfen gem. § 32 Abs. 1 S. 2 BDSG zur Aufdeckung von Straftaten nur dann erhoben, verarbeitet oder genutzt werden, wenn tatsächliche Anhaltspunkte (begründeter Verdacht) dafür vorliegen, dass der Beschäftigte eine Straftat begangen hat, die *im Zusammenhang mit dem Beschäftigungsverhältnis* steht. Entscheidend ist hierbei, dass der Arbeitgeber entsprechende Anhaltspunkte dokumentieren muss. Auch muss die Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten des Beschäftigten *zur Aufdeckung dieser Straftat erforderlich* sein. Darüber hinaus darf das schutzwürdige

²³ § 32 Abs. 1 Satz 2 BDSG spricht davon, dass zur Aufdeckung von Straftaten personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden dürfen, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass Klarer kann der Gesetzgeber seinen Willen, dass für diese Zwecke nur diese Vorschrift und insbesondere keine anderen generalklauselartigen Bestimmungen mit offenen Wertungsmöglichkeiten für den Rechtsanwender einschlägig sein sollen, kaum zum Ausdruck bringen.

Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht *überwiegen*; insbesondere darf Art und Ausmaß im Hinblick auf den Anlass nicht *unverhältnismäßig* sein.²⁴

- Die Novelle des BDSG brachte auch erhebliche Änderungen des bisherigen Sanktionsinstrumentariums bei Datenschutzverstößen mit sich. Der bisher gesetzlich vorgesehene Bußgeldrahmen bei Datenschutzverstößen ist erhöht worden auf Maximalsummen von 50.000 € für Verstöße gegen Verfahrensvorschriften und von 300.000 € für Verstöße gegen materielle Datenschutzbestimmungen. Neu hinzugekommen ist auch eine Regelung, wonach diese Höchstbeträge im Einzelfall überschritten werden können; dies soll insbesondere die Abschöpfung des wirtschaftlichen Vorteils ermöglichen, den die verantwortliche Stelle aus den Datenschutzverstößen erlangt hat.

Bislang waren die Aufsichtsbehörden darauf beschränkt, bei erkannten Datenschutzverstößen Bußgelder gegen die verantwortliche Stelle zu verhängen. Eine Beanstandung gesetzeswidriger Datenverarbeitung war nicht vorgesehen. Nunmehr ermächtigt **§ 38 Abs. 5 S. 1 BDSG** die Aufsichtsbehörden ausdrücklich dazu, nicht nur die Maßnahmen zur Beseitigung festgestellter Verstöße anzuordnen, sondern sogar im Falle schwerwiegender Mängel die Datenerhebung und Verwendung oder den Einsatz einzelner Verarbeitungsverfahren insgesamt zu untersagen.

- Neu ist auch die Informationspflicht, die eine verantwortliche Stelle trifft, wenn Daten unrechtmäßig Dritten zur Kenntnis gelangt sind, also eine sog. Datenschutzpanne eingetreten ist (vgl. § 42 a BDSG).

§ 42 a BDSG statuiert eine Informationspflicht von Unternehmen, wenn bei diesen eine sog. *Datenschutzpanne* eingetreten ist. Diese Datenschutzpanne muss allerdings die in § 42 a BDSG aufgeführten sensiblen Daten betreffen. Eine Datenschutzpanne liegt vor, wenn die sensiblen Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind. Zudem müssen dem Betroffenen schwerwiegende Beeinträchtigung

²⁴ Zu diesem Themenkomplex existiert ein Entwurf eines Beschäftigungsdatschutzgesetzes, der intensiv diskutiert wird. Mit Änderungen auf diesem Gebiet ist daher zu rechnen.

gungen materieller oder immaterieller Art drohen.²⁵ Die verantwortliche Stelle muss in einem solchen Fall die zuständige Aufsichtsbehörde und den Betroffenen unverzüglich benachrichtigen. Die Vorschrift des § 42 a BDSG regelt darüber hinaus den genauen Inhalt und mögliche Formen der Information. Der betriebliche Datenschutzbeauftragte ist in das Verfahren einzubeziehen.

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

2.2.1.3 Novelle III - Gesetz vom 29. Juli 2009

Der Bundestag hat zudem im Sommer 2009 auch die Novelle III zu Auskunftspflichten von Auskunftgebern und der kreditgebenden Wirtschaft beschlossen²⁶. Dies war erforderlich, um die EU-Verbraucherkreditrichtlinie umzusetzen. Die entscheidenden Änderungen betrafen das BGB aber auch das BDSG. § 29 BDSG wurde um zwei Absätze erweitert. Diese Erweiterung begründet neue Verhaltenspflichten von Datenbankbetreibern, die Auskünfte zur Bewertung der Kreditwürdigkeit potentieller Darlehensnehmer erteilen. Inhaltliche Vorgaben ergeben sich aus dem mit der Novelle I zeitgleich geschaffenen § 28b BDSG. Die Änderungen der Novelle III sind am 11. Juni 2010 in Kraft getreten.

2.2.2. Telekommunikationsgesetz (TKG)

Im Zusammenhang mit dem Gesetz, das die BDSG Novelle II²⁷ des Jahres 2009 enthielt²⁸, wurden auch entsprechende Anpassungen in datenschutz-

²⁵ Zu dieser Vorgabe dürfte eine Änderung im Hinblick auf die europäische Richtlinie 2009/136/EG erforderlich werden, die bis zum 25.05.2011 in nationales Recht umgesetzt werden muss. Vgl. hierzu oben 2.1.4.

²⁶ Gesetz zur Umsetzung der Verbraucherkreditrichtlinie, des zivilrechtlichen Teils der Zahlungsdiensterichtlinie sowie zur Neuordnung der Vorschriften über das Widerrufs- und Rückgaberecht vom 29.07.2009, BGBl. I 2009, S. 2355.

²⁷ Vgl. oben 2.2.1.2.

²⁸ Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 14. August 2009, BGBl. I 2009, S. 2814

rechtlicher Hinsicht im TKG vorgenommen. Diese betrafen einerseits den Fall, dass bei einem Diensteanbieter gespeicherte Bestandsdaten oder Verkehrsdaten unrechtmäßig übermittelt wurden oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind. § 93 Abs. 3 TKG sieht hierfür seither die entsprechende Anwendung des § 42a BDSG²⁹ vor. In § 95 Abs. 5 TKG wurde zudem ein den Vorgaben des ebenfalls neuen § 28 Abs. 3b BDSG angeglichenes Kopplungsverbot niedergelegt.³⁰ Insoweit liegt eine weitgehende Parallelität der Regelungen vor, was wegen der Ähnlichkeit der geregelten Lebenssachverhalte prinzipiell zu begrüßen ist.

Die bedeutendste Veränderung in datenschutzrechtlicher Hinsicht erfolgte aber zur Umsetzung der Vorgaben der bereits oben genannten Richtlinie 2006/24/EG³¹. Die Umsetzung der dort vorgesehenen Vorratsdatenspeicherung hatte eine durchgreifende Änderung des Telekommunikationsrechts zur Folge. Zu diesem Zwecke wurde das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG³² beschlossen, das am 01. Januar 2008 in Kraft trat.

Durch dieses Gesetz wurden zur Neuregelung der Telekommunikationsüberwachung die Vorschriften der §§ 113 a und 113 b in das TKG eingefügt.

§ 113 a TKG verpflichtete Anbieter von öffentlich zugänglichen Telekommunikationsdiensten, praktisch sämtliche Verkehrsdaten von Telefondiensten, E-Mail-Diensten und Internetdiensten vorsorglich und anlasslos zu speichern. Die Speicherungspflicht erstreckte sich im Wesentlichen auf alle Angaben, die erforderlich sind, um zu rekonstruieren, wer wann wie lange mit wem von wo aus kommuniziert hat oder zu kommunizieren versucht hat. Nicht zu speichern war demgegenüber der Inhalt der Kommunikation, und damit auch, welche Internetseiten von den Nutzern aufgerufen wurden. Nach Ablauf der Speicherungspflicht von sechs Monaten waren diese Daten innerhalb eines Monats zu löschen.

§ 113 b TKG benannte mögliche Zwecke, für die diese Daten verwendet werden durften. Die Vorschrift verstand sich dabei als Scharniernorm: Sie enthielt selbst keine Ermächtigung zur Datenabfrage, sondern bezeichnete nur grobmaschig allgemein mögliche Nutzungszwecke, die durch fachrechtliche Regelungen des Bundes und der Länder konkretisiert werden sollten. In Satz 1 HS 1 wurden dabei die möglichen Zwecke der unmittelbaren Nut-

²⁹ Vgl. oben 2.2.1.2. zu § 42 a BDSG.

³⁰ Vgl. oben 2.2.1.2. zu § 28 Abs. 3b BDSG.

³¹ Vgl. oben 2.1.2.

³² BGBl. I 2007, S. 3198.

zung der Daten aufgelistet: Die Verfolgung von Straftaten, die Abwehr von erheblichen Gefahren für die öffentliche Sicherheit und die Erfüllung nachrichtendienstlicher Aufgaben.

Halbsatz 2 erlaubte darüber hinaus die mittelbare Nutzung der Daten für Auskünfte nach § 113 Abs. 1 TKG in Form eines Auskunftsanspruchs gegenüber den Diensteanbietern zur Identifizierung von IP- Adressen. Behörden konnten danach, wenn sie etwa durch Anzeige oder durch eigene Ermittlungen eine IP- Adresse schon kannten, Auskunft verlangen, welchem Anschlussnehmer diese Adresse zugeordnet war.

Gegen diese Regelungen wurde von verschiedenen Seiten Verfassungsbeschwerde erhoben. Die Verfassungsbeschwerden richteten sich gegen §§ 113 a, 113 b TKG und gegen § 100 g StPO, soweit danach die Erhebung von nach § 113 a TKG gespeicherten Daten zulässig war.³³

Die Beschwerdeführer sahen durch die Vorratsdatenspeicherung vor allem das Telekommunikationsgeheimnis und das Recht auf informationelle Selbstbestimmung verletzt. Sie hielten die anlasslose Speicherung aller Telekommunikationsverbindungen für unverhältnismäßig. Insbesondere machten sie geltend, dass sich aus den gespeicherten Daten Persönlichkeits- und Bewegungsprofile erstellen ließen. Eine Beschwerdeführerin, die einen Internetanonymisierungsdienst anbietet, rügt zudem, die mit der Speicherung verbundenen Kosten würden die Anbieter von Telekommunikationsdiensten unverhältnismäßig in ihrer Berufsfreiheit beeinträchtigen.

Das Bundesverfassungsgericht hat hierzu in seinem Urteil vom 02. März 2010³⁴ entschieden, dass die oben genannten Regelungen des TKG und der StPO über die Vorratsdatenspeicherung mit Art. 10 Abs. 1 GG nicht vereinbar sind. Zwar ist eine Speicherpflicht in dem vorgesehenen Umfang nicht von vornherein schlechthin verfassungswidrig. Es fehlte aber an einer dem Verhältnismäßigkeitsgrundsatz entsprechenden Ausgestaltung. Die angegriffenen Vorschriften gewährleisteten weder eine hinreichende Datensicherheit, noch eine hinreichende Begrenzung der Verwendungszwecke der Daten. Auch genühten sie nicht in jeder Hinsicht den verfassungsrechtlichen Transparenz- und Rechtsschutzanforderungen. Die Regelungen wurden damit insgesamt für verfassungswidrig und nichtig erklärt.³⁵

³³ Vgl. Pressemitteilung des Bundesverfassungsgerichtes Nr. 11/2010 vom 02. März 2010.

³⁴ Urteil des BVerfG vom 02. März 2010, BVerfGE 125, 260 ff.,

³⁵ Da das Urteil erst am 02. März 2010 und damit außerhalb des Berichtszeitraums ergangen ist, beschränkt sich die Darstellung auf die wesentlichen Kernaussagen.

2.2.3. Telemediengesetz (TMG)

Eine in datenschutzrechtlicher Hinsicht maßgebliche Veränderung des TMG erfolgte durch die Aufhebung des ursprünglichen § 12 Abs. 3 TMG und damit des dort niedergelegten Koppelungsverbot.³⁶ Nach dieser über § 47 Abs. 1 RStV auch auf den Rundfunk anwendbaren Bestimmung durfte die Bereitstellung von Diensten nicht von der Einwilligung des Nutzers in die Verwendung seiner Daten für andere Zwecke abhängig gemacht werden, wenn dem Nutzer ein anderer Zugang zu diesen Diensten nicht oder in nicht zumutbarer Weise möglich war.

Nach der Streichung dieser Vorschrift enthält das TMG keine eigenständige Regelung des Koppelungsverbot mehr, sondern verweist allgemein auf die jeweils geltenden Vorschriften für den Schutz personenbezogener Daten und damit letztendlich zumeist auf § 28 Abs. 3b BDSG³⁷. Das dortige Koppelungsverbot schließt eine Einwirkung auf den Nutzer nur dann aus, wenn ein anderer Zugang zu gleichwertigen vertraglichen Leistungen nicht oder in nicht zumutbarer Weise möglich ist. Unter der Geltung des § 12 Abs. 3 TMG a.F. bezog sich diese Vergleichsüberlegung noch auf den Zugang zu diesen Diensten.

Für den Rundfunk war diese Unterscheidung deshalb von nicht zu unterschätzender Bedeutung, weil vor dem Hintergrund der verfassungsrechtlichen Zielvorstellung einer vom Rundfunk abzubildenden möglichst großen Meinungsvielfalt, die Verweigerung des Zugang zu bestimmten Inhalten und Meinungen und der Verweis auf andere wenn auch gleichwertige Dienste und Meinungen ggf. eine Zielverfehlung darstellen kann.

Im Übrigen wurde mit dem bereits erwähnten Gesetz, das die BDSG Novelle II³⁸ des Jahres 2009 enthielt, für Datenpannen die in § 42a BDSG vorgesehene Rechtsfolge übernommen, indem im neuen § 15a TMG für dort beschriebene Fälle § 42a BDSG für entsprechend anwendbar erklärt wurde.

2.2.4. Allgemeines Gleichbehandlungsgesetz (AGG)

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

³⁶ Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 14. August 2009, BGBl. I 2009, S. 2814, (das auch die BDSG Novelle II des Jahres 2009 enthielt).

³⁷ In Ausnahmefällen mag auch der weitgehend inhaltsgleiche § 95 Abs. 5 TKG anwendbar sein.

³⁸ Vgl. oben 2.2.1.2.

2.2.5. Informationsfreiheitsgesetz des Bundes (IFG)

Auch hier gab es im Berichtszeitraum keine datenschutzrechtlich relevanten Änderungen.

2.2.6. Gesetz über das Verfahren des elektronischen Entgeltnachweises (sog. ELENA-Verfahrensgesetz) vom 28. März 2009

Am 28. März 2009 wurde das Gesetz über das Verfahren des elektronischen Entgeltnachweises (sog. ELENA-Verfahrensgesetz)³⁹ beschlossen. Das Gesetz trat am 1. Januar 2010 in Kraft.

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

In der ELENA-Datenbank werden ab dem 1. Januar 2010 Daten zum Einkommen der Betroffenen gespeichert, die bislang in Antragsverfahren vor Sozialbehörden für die Prüfung etwaiger Ansprüche auf Sozialleistung notwendig sind. Die gespeicherten Daten sollen erst ab dem 1. Januar 2012 von den ausdrücklich dazu befugten Stellen einzelfallbezogen abgerufen werden können, sofern der betroffene Antragsteller den Abruf mit seiner individuellen elektronischen Signaturkarte freigegeben hat. Der Arbeitgeber hat auf der Entgeltbescheinigung auf die Übermittlung der Daten hinzuweisen wie auch darauf, dass ein Auskunftsrecht gegenüber der zentralen Speicherstelle besteht.

Mit diesem Verfahren des elektronischen Entgeltnachweises wird wiederum aufgrund eines Gesetzes eine große zentrale Datensammlung mit personenbezogenen Daten geschaffen, die schon alleine für sich betrachtet, aber vor allem im Zusammenspiel mit anderen Daten aufschlussreiche Rückschlüsse weit jenseits der Frage des individuellen Gehalts des Betroffenen erlauben dürfte, ohne dass der einzelne Bürger dazu einen Anlass geboten hätte. Hintergrund hierfür ist, dass nicht nur die tatsächlichen Gehaltszahlungen, sondern auch Schwankungen des regelmäßigen Gehaltes und die hierfür maßgeblichen Gründe angegeben, zentral gesammelt und in einer Datenbank gespeichert werden sollen. Als besonders problematisch wurden Angaben über

³⁹ BGBl. I 2009, 634ff

krankheits- oder gar arbeitskampfbedingte Ausfalltage angesehen.

Datenschützer hatten während des gesamten Entstehungsprozesses erhebliche Bedenken angemeldet. Zentrale Kritikpunkte waren einerseits, dass die Daten zentral, anlasslos und sogar auch zu Personen erhoben werden, bei denen sehr unwahrscheinlich ist, dass die Daten tatsächlich jemals gebraucht werden könnten, so dass wiederum eine neue Form von Vorratsdatenspeicherung vorgeschrieben wird. Andererseits wurde aber auch die Detailtiefe der Datenabfrage problematisiert.

In der Zwischenzeit wurde am 31.03.2010 eine Verfassungsbeschwerde gegen den elektronischen Einkommensnachweis ELENA in Karlsruhe eingereicht. Daneben findet eine politische Diskussion vor allem auch zu den besonders vehement kritisierten Angaben zu Fehlzeiten und arbeitsrechtlichen Vorgängen statt.

Juristisch gesehen führt jedoch an ELENA seit Juli 2010 zunächst kein Weg mehr vorbei. Ansonsten würden Arbeitgeber gegen existierende gesetzliche Meldepflichten verstoßen. Ein solcher Verstoß stellt eine Ordnungswidrigkeit dar, die mit einem Bußgeld von bis zu 25.000 Euro belegt werden kann.

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

Am 1. Januar 2009 ist die Novellierung des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten⁴⁰ in Kraft getreten.

Die Änderungen im BKA-Gesetz waren darauf ausgerichtet, den Beamten des Bundeskriminalamtes umfangreiche neue Befugnisse einzuräumen, um die Bekämpfung des internationalen Terrorismus zu verbessern.⁴¹ Neben der Online-Durchsuchung regeln die neuen Vorschriften des BKA-Gesetzes u.a. die Rasterfahndung, den Einsatz verdeckter Ermittler, akustische und optische Überwachung von Wohnungen und die Telekommunikationsüberwachung.

Zahlreiche Institutionen bis hin zum Bundesbeauftragten für den Datenschutz, vor allem aber auch Journalisten- und Medienverbände haben zu dem Gesetzentwurf zumeist kritisch Stellung genommen. Sie kritisierten die

⁴⁰ Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt vom 25.12.2008, BGBl I 2008, S. 3083.

⁴¹ Vgl. § 20a - § 20x BKAG.

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

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

2.2.8. Urteil des BVerfG zur Online-Durchsuchung

Das Bundesverfassungsgericht hatte aufgrund von verschiedenen Verfassungsbeschwerden über die Zulässigkeit von Online-Durchsuchungen zu entscheiden. Der erste Senat des Bundesverfassungsgerichts hat mit Urteil vom 27. Februar 2008⁴² die Vorschriften zur Online-Durchsuchung sowie zur Aufklärung des Internets des Verfassungsschutzgesetzes Nordrhein-Westfalen (VSG) für verfassungswidrig erklärt.

§ 5 Abs. 2 Nr. 11 S. 1 Alt 2 VSG regelte den heimlichen Zugriff auf informationstechnische Systeme („Online-Durchsuchung“). Das Bundesverfassungsgericht sah hierin eine Verletzung des allgemeinen Persönlichkeitsrechts in seiner besonderen Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Die Vorschrift entsprach nach den Feststellungen des BVerfG insbesondere nicht dem Gebot der Verhältnismäßigkeit. In Anbetracht der Schwere des Eingriffs sei die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden könnten, nur dann zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestünden. Zudem

⁴² Urteil des BVerfG vom 27. Februar 2008, BVerfGE 120, 274 ff.

sei der Eingriff grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen. Diesen Anforderungen sei die oben genannte Vorschrift des VSG gerade nicht gerecht geworden. Darüber hinaus fehlte es auch an hinreichenden gesetzlichen Vorkehrungen, um Eingriffe in den absolut geschützten Kernbereich privater Lebensgestaltung zu vermeiden.⁴³

Die Nutzung informationstechnischer Systeme sei für die Persönlichkeitsentfaltung vieler Bürger von zentraler Bedeutung, begründe aber gleichzeitig neuartige Gefährdungen der Persönlichkeit. Eine Überwachung der Nutzung solcher Systeme und eine Auswertung der auf den Speichermedien befindlichen Daten könne weit reichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zur Profilbildung ermöglichen. Hieraus folge ein grundrechtlich erhebliches Schutzbedürfnis. Die Gewährleistungen der Art. 10 GG (Telekommunikationsgeheimnis) und Art. 13 GG (Unverletzlichkeit der Wohnung) wie auch die bisher in der Rechtsprechung des Bundesverfassungsgerichts entwickelten Ausprägungen des allgemeinen Persönlichkeitsrechts trügen dem durch die Entwicklung der Informationstechnik entstandenen Schutzbedürfnis nicht hinreichend Rechnung.⁴⁴

Aufgrund der sich aus diesen Erwägungen ergebenden Regelungslücke hat das Bundesverfassungsgericht in seinem Urteil zum ersten Mal entschieden, dass das allgemeine Persönlichkeitsrecht dem Schutzbedarf über seine bisher anerkannten Ausprägungen hinaus dadurch Rechnung trägt, dass es die *Integrität und Vertraulichkeit informationstechnischer Systeme* gewährleistet. Dieses Grundrecht ist anzuwenden, wenn die Eingriffsermächtigung Systeme erfasst, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, so dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten.⁴⁵

Die angegriffene Vorschrift ermächtigt zu Grundrechtseingriffen von besonders hoher Intensität. Angesichts der Schwere des Eingriffs, kann dieser nur verfassungsrechtlich zulässig sein, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.⁴⁶ Zudem muss der Zugriff unter dem Vorbehalt richterlicher Anordnung stehen. Diesen Anforderungen genüge die Vorschrift gerade nicht.

⁴³ Pressemitteilung Nr. 22/2008 vom 27. Februar 2008.

⁴⁴ BVerfGE 120, 274 ff.

⁴⁵ Vgl. ebd.

⁴⁶ Vgl. ebd.

Es fehlte zudem insbesondere auch an hinreichenden gesetzlichen Vorkehrungen, um Eingriffe in den absolut geschützten Kernbereich privater Lebensgestaltung zu vermeiden. Eine Ermittlungsmaßnahme wie der Zugriff auf ein informationstechnisches System, mittels dessen die auf dem Zielsystem vorhandenen Daten umfassend erhoben werden können, schafft gegenüber anderen Überwachungsmaßnahmen die gesteigerte Gefahr, dass Daten höchstpersönlichen Inhalts erhoben werden.

Der verfassungsrechtlich gebotene Kernbereichsschutz lässt sich im Rahmen eines zweistufigen Schutzkonzepts gewährleisten: Die gesetzliche Regelung hat darauf hinzuwirken, dass die Erhebung kernbereichspezifischer Daten soweit wie informationstechnisch und ermittlungstechnisch möglich unterbleibt. Insbesondere sind verfügbare informationstechnische Sicherungen einzusetzen. Ist praktisch unvermeidbar, Informationen zur Kenntnis zu nehmen, bevor ihr Kernbereichsbezug bewertet werden kann, muss für hinreichenden Schutz in der Auswertungsphase gesorgt werden. Insbesondere müssen aufgefundene und erhobene Daten mit Kernbereichsbezug unverzüglich gelöscht und ihre Verwertung ausgeschlossen werden. Auch diesen Anforderungen genügt die Vorschrift nicht.⁴⁷

Daneben verletzte nach der Entscheidung des BVerfG aber auch die Ermächtigung zum heimlichen Aufklären des Internets in § 5 Abs. 2 Nr. 11 S. 1 Alt. 1 VSG die Verfassung und wurde für nichtig erklärt. Das heimliche Aufklären des Internets greife in das Telekommunikationsgeheimnis ein, wenn die Verfassungsschutzbehörde zugangsgesicherte Kommunikationsinhalte überwache, indem sie Zugangsschlüssel nutze, die sie ohne oder gegen den Willen der Kommunikationsteilnehmer erhoben habe. Ein derart schwerer Grundrechtseingriff setze grundsätzlich zumindest die Normierung einer qualifizierten materiellen Eingriffsschwelle voraus. Daran fehle es hier. Die Norm lasse nachrichtendienstliche Maßnahmen in weitem Umfang im Vorfeld konkreter Gefährdungen zu ohne Rücksicht auf das Gewicht der möglichen Rechtsgutverletzungen und auch gegenüber unbeteiligten Dritten. Zudem enthalte diese Norm auch keine Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung.⁴⁸

Maßnahmen nach der oben genannten Vorschrift könnten sich in bestimmten Fällen als Eingriff in das Telekommunikationsgeheimnis (Art. 10 GG) darstellen, der verfassungsrechtlich nicht gerechtfertigt sei.

Verschafft sich der Staat Kenntnis von den Inhalten einer über die Kommunikationsdienste des Internet geführten Fernkommunikation auf dem dafür

⁴⁷ BVerfGE 120, 274 ff.

⁴⁸ Vgl. ebd.

technisch vorgesehenen Weg, so liege darin ein Eingriff in Art. 10 Abs. 1 GG, wenn die staatliche Stelle hierzu nicht durch Kommunikationsbeteiligte autorisiert sei. Dies sei der Fall, wenn die Verfassungsschutzbehörde zugangsgesicherte Kommunikationsinhalte überwachten, indem sie Zugangsschlüssel nutzten, die sie ohne oder gegen den Willen der Kommunikationsbeteiligten erhoben hätten.

Stehe im Vordergrund einer staatlichen Ermittlungsmaßnahme dagegen nicht der unautorisierte Zugriff auf die Telekommunikation, sondern die Enttäuschung des personengebundenen Vertrauens in den Kommunikationspartner, so liege darin kein Eingriff in Art. 10 Abs. 1 GG. Daher sei ein Eingriff in das Telekommunikationsgeheimnis zu verneinen, wenn etwa ein Teilnehmer eines geschlossenen Chats der für die Verfassungsschutzbehörde handelnden Person seinen Zugang freiwillig zur Verfügung stelle und die Behörde in der Folge diesen Zugang nutze. Erst recht scheide ein Eingriff in das Telekommunikationsgeheimnis aus, wenn die Behörde allgemein zugängliche Inhalte erhebe, etwa indem sie offene Diskussionsforen und nicht zugangsgesicherte Webseiten einsehe.⁴⁹

Die von der oben genannten Vorschrift ermöglichten Eingriffe auch in Art. 10 Abs. 1 GG seien daher verfassungsrechtlich nicht gerechtfertigt.

2.3. Bayerisches Landesrecht

2.3.1. Art. 21 a BayDSG

Bereits im letzten Tätigkeitsbericht war auf den Beschluss des Bundesverfassungsgerichts hingewiesen worden, wonach die Videoüberwachung öffentlicher Plätze, auch wenn sie der Sicherung eines Kunstwerks auf einem städtischen Platz diene, nicht auf Art. 16 Abs. 1 bzw. Art. 17 Abs. 1 BayDSG gestützt werden könne.⁵⁰

Eine solche Maßnahme diene der Ahndung von unerwünschten Verhaltensweisen sowie zur Abschreckung, und stelle einen Eingriff von erheblichem Gewicht in das betroffene Grundrecht dar. Dies ergebe sich bereits daraus, dass es sich um einen verdachtslosen Eingriff mit großer Streubreite handle, bei dem zahlreiche Personen in den Wirkungsbereich der Maßnahme einbezogen würden, die in keiner Beziehung zu einem konkreten Fehlverhalten stünden und den Eingriff nicht durch ihr Verhalten veranlasst hätten.

⁴⁹ BVerfGE 120, 274 ff.

⁵⁰ Beschluss der 1. Kammer des Ersten Senats des Bundesverfassungsgerichts vom 23. Februar 2007, DVBl. 2007, 497 = NVwZ 2007, 688.

Für einen solch massiven Eingriff fehlte bislang eine hinreichende Ermächtigungsgrundlage. Mit dem Änderungsgesetz vom Juni 2008⁵¹ wurde daher die Vorschrift Art. 21 a BayDSG zur Videoüberwachung eingeführt.

Mit Art. 21 a BayDSG wurde für die Erhebung (Videobeobachtung) und die Speicherung (Videoaufzeichnung) personenbezogener Daten nun eine spezielle Rechtsgrundlage geschaffen. Die Vorschrift gilt für alle bayerischen öffentlichen Stellen.

Die Videoüberwachung ist nur zulässig, wenn sie im Rahmen der Erfüllung öffentlicher Aufgaben oder in Ausübung des Hausrechts erforderlich ist, um Leben, Gesundheit, Freiheit oder Eigentum von Personen, die sich im Bereich öffentlicher Einrichtungen, öffentlicher Verkehrsmittel, von Dienstgebäuden oder sonstigen baulichen Anlagen öffentlicher Stellen oder in deren unmittelbarer Nähe aufhalten⁵², oder um die genannten Einrichtungen selbst oder die dort oder in unmittelbarer Nähe befindlichen Sachen⁵³ zu schützen. Es dürfen außerdem keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen der Betroffenen beeinträchtigt werden.

Die Videoüberwachung und die erhebende Stelle sind durch geeignete Maßnahmen erkennbar zu machen.⁵⁴

Die Daten dürfen für den Zweck verarbeitet und genutzt werden, für den sie erhoben worden sind, für einen anderen Zweck nur, soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von Straftaten erforderlich ist.⁵⁵

Danach sind die auf diese Weise erstellten Videoaufzeichnungen und daraus gefertigte Unterlagen spätestens drei Wochen nach der Datenerhebung zu löschen, soweit sie nicht zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von Straftaten oder zur Geltendmachung von Rechtsansprüchen benötigt werden.⁵⁶

Für Videoaufzeichnungen ist vom behördlichen Datenschutzbeauftragten der öffentlichen Stelle eine datenschutzrechtliche Freigabe zu erteilen.⁵⁷

⁵¹ Gesetz vom 10. Juni 2008, BayGVBl vom 16.06.2008, S. 315.

⁵² Vgl. Art. 21 a Abs. 1 Nr. 1 BayDSG.

⁵³ Vgl. Art. 21 a Abs. 1 Nr. 2 BayDSG.

⁵⁴ Vgl. Art. 21 a Abs. 2 BayDSG.

⁵⁵ Vgl. Art. 21 a Abs. 3 BayDSG.

⁵⁶ Vgl. Art. 21 a Abs. 5 BayDSG.

⁵⁷ Vgl. Art. 21 a Abs. 6 BayDSG.

2.3.2. Rundfunkstaatsvertrag

Im Berichtszeitraum sind zwar der 10., 11. und der 12. Rundfunkänderungsstaatsvertrag in Kraft getreten; datenschutzrechtlich bedeutsame Regelungen sind von diesen Änderungen jedoch nicht betroffen.

2.3.3. Bayerisches Mediengesetz

Auch die im Berichtszeitraum erfolgten Änderungen im Bayerischen Mediengesetz entfalteten keine datenschutzrechtlichen Wirkungen.

3. Funktion des Beauftragten für den Datenschutz

Mit Art. 20 BayMG als bereichsspezifischer 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 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 S. 2 BayMG die Einhaltung der Vorschriften des BayMG sowie anderer Vorschriften über den Datenschutz bei der Landeszentrale und bei den Anbietern umfassend⁵⁸, und zwar auch, soweit es sich um Verwaltungsangelegenheiten handelt.⁵⁹ Mit dieser umfassenden Zuständigkeit für alle Aufgaben bei der Landeszentrale und den Anbietern trägt das BayMG den verfassungsrechtlichen Anforderungen an einen rundfunkrechtlichen Datenschutz Rechnung.⁶⁰

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.⁶¹

⁵⁸ 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.

⁵⁹ Vgl. Art. 20 Abs. 3 S. 3 BayMG.

⁶⁰ 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.“

⁶¹ Vgl. insbesondere Art. 20 Abs. 4 BayMG.

Der Beauftragte für den Datenschutz bei der Landeszentrale ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Ein solcher unabhängiger Datenschutzbeauftragter ist vor allem im Hinblick auf die Überwachung der Datenschutzregelung nach Art. 20 Abs. 2 BayMG für den journalistisch-redaktionellen Bereich notwendig und zweckmäßig. Da der Datenschutzbeauftragte unabhängig und nur dem Gesetz unterworfen ist, können keine Weisungen, insbesondere auch nicht vom Präsidenten oder dem Verwaltungsrat erteilt werden, die sich auf seine inhaltliche Aufgabenerfüllung beziehen. Die Stellung des Datenschutzbeauftragten bei der Landeszentrale entspricht damit der eines Richters.

Die Ausgestaltung der Datenschutzaufsicht nach dem BayMG entspricht somit auch zweifelsfrei den Anforderungen der EU-Datenschutzrichtlinie⁶², die in Art. 28 Abs. 1 den Mitgliedsstaaten auferlegt, datenschutzrechtliche Kontrollstellen zu schaffen, die die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahrnehmen. Die Erfüllung dieser Vorgabe war in der Vergangenheit für die Aufsicht über den nicht-staatlichen Bereich in der Bundesrepublik nicht unumstritten. Die Europäische Kommission hatte am 5. Juli 2005 ein Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland eingeleitet, in dem die Kommission monierte, dass die Datenschutzaufsicht über die Privatwirtschaft, wie sie zum damaligen Zeitpunkt organisiert war, nicht in allen Fällen über die geforderte „völlige Unabhängigkeit“ verfüge. Das Verfahren wurde in der Zwischenzeit vom Europäischen Gerichtshof durch Urteil⁶³ vom 09. März 2010 im Sinne der Europäischen Kommission entschieden.⁶⁴ Die Gestaltung nach dem BayMG wurde dabei nicht angesprochen.

Der Beauftragte für den Datenschutz bei der Landeszentrale untersteht nach Art. 20 Abs. 3 S. 7 BayMG intern der Dienstaufsicht des Verwaltungsrates. Zur Dienstaufsicht sind nur arbeitsrechtliche Belange zu zählen. Eine Delegation der Dienstaufsicht an andere Organe der Landeszentrale oder leitende Angestellte ist nicht möglich. Insbesondere besteht keine Einordnung des Beauftragten für den Datenschutz bei der Landeszentrale in den durch den Präsidenten der Landeszentrale geleiteten Verwaltungsaufbau. Der Präsident beruft zwar den Beauftragten für den Datenschutz bei der Landeszentrale, bedarf hierfür aber der Zustimmung des Verwaltungsrates.⁶⁵

Im Übrigen bestehen für den Präsidenten oder für von diesem beauftragte Personen keine Aufsichtsbefugnisse über oder sonstige Beeinflussungsmöglichkeiten hinsichtlich des Beauftragten für den Datenschutz bei der Landeszentrale. Vielmehr führt dieser in datenschutzrechtlicher Hinsicht die Aufsicht über die Landeszentrale und den durch den Präsidenten geleiteten Verwaltungsaufbau. Es besteht lediglich eine interne Dienstaufsicht, die durch den Verwaltungsrat wahrgenommen wird.

⁶² RL 95/46/EG, ABl. EG v.23.11.1995, Nr. L 281/31.

⁶³ Urteil des EuGH vom 09. März 2010, Az: C- 518/07.

⁶⁴ Vgl. hierzu oben 2.1.3.

⁶⁵ Vgl. Art. 20 Abs. 3 Satz 1 BayMG.

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

4. Datenschutz in der Landeszentrale

4.1. Allgemeines

4.1.1. Datenschutzrechtliche Freigabe automatisierter Verfahren nach Art. 26 BayDSG

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

Im Berichtszeitraum ist kein neues derartiges Verfahren eingeführt worden.

4.1.2. Verzeichnisse 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 Verzeichnisse wird jährlich fortgeschrieben.

Obwohl nach Art. 27 BayDSG die vormals bestehende Pflicht zur Führung eines Anlageverzeichnisses weggefallen ist, ist mit der EDV-Abteilung vereinbart, dass dieses Anlageverzeichnis in gewisser Weise fortgeführt wird. Ein Verwaltungsaufwand entsteht hierdurch nicht, da die eingesetzte Hardware sowie die Peripherie-Geräte weiter inventarisiert und als Anlagevermögen aktiviert werden und daher im Anlagespiegel gem. § 268 Abs. 2 HGB geführt werden müssen. Der Anlagespiegel unterstützt insoweit auch Planungen bei der Entwicklung von Konzepten auf dem Gebiet der Datensicherheit.

4.2. Verwaltungsgebäude der Landeszentrale

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

Nennenswerte Auffälligkeiten konnten im Berichtszeitraum nicht festgestellt werden.

4.3. Mitarbeiterschulung

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.

5. Datenschutz bei den Anbietern und Tochtergesellschaften der Landeszentrale

Im Zentrum meiner Tätigkeit stand einerseits 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.

Im Jahr **2008** standen einerseits Fragen zum organisatorischen Ablauf und zur Bearbeitung datenschutzrechtlicher Anfragen im Vordergrund. So stellte sich u.a. die Frage, ob und wann datenschutzrechtliche Beschwerden auch vom zuständigen Kundenbetreuer beantwortete bzw. automatisch an den jeweiligen Datenschutzbeauftragten weitergeleitet werden sollten oder wann es ratsam erscheint zu empfehlen, dass der Kunde sich nochmals in schriftlicher Form direkt an den Datenschutzbeauftragten wenden sollte.

Einen weiteren Schwerpunkt bildeten andererseits Beschwerden über Anbietern, die auf Verwechslungen von Kundendaten z.B. bei der Eingabe der Daten in informationstechnische Systeme bzw. auf Fehlern im Zusammenhang mit der Verarbeitung von Daten beruhten.

Beschwerden über unerwünschte Werbung per E-Mail oder per Post waren im Jahr 2008 ebenfalls vermehrt eingegangen, erreichten aber ein noch überschaubares Maß. Dabei war es für die Beschwerdeführer gelegentlich auch bedeutsam, dass eruiert wurde, woher die jeweiligen Daten stammten und wie sie durch den Anbieter erworben wurden bzw. zu ihm gelangten, insbesondere wenn die Kunden bis dahin in keinerlei vertraglichem Verhältnis zum Anbieter gestanden hatten.

Es stellten sich zudem über Beschwerden von Kunden wiederholt Fragen nach der Zulässigkeit der Übermittlung von Daten an Dritte, vor allem wenn die Betroffenen davon ausgingen, dass weder ihre Einwilligung noch ein ausreichend schutzwürdiges Interesse des übermittelnden Unternehmens vorlag. Neben datenschutzrechtlichen Aspekten waren in diesem Zusammenhang insbesondere auch zivilrechtliche Fragen zu bewerten. Trotz der Veränderungen der maßgeblichen Vorschriften des BDSG durch die BSDG-Novelle II mit Gesetz vom 14.08.2009⁶⁶ sind diese Fragen nach wie vor noch aktuell und hatten auch Auswirkungen auf Anfragen im Jahr 2009.

Datenschutzrechtlich geprüft werden musste auch, ob und unter welchen Umständen die Weitergabe von Inkassodaten an Auskunftsteilen zulässig sein kann. In der Zwischenzeit hat der Gesetzgeber die insoweit maßgeblichen Vorgaben präzisiert und einige Fragen auch ausdrücklich in § 28a BDSG geregelt.

Im Jahr **2009** hat sich die Anzahl der Beschwerden insgesamt nochmals verdoppelt.

⁶⁶ Vgl. oben 2.2.1.2.

Wie bereits im Jahr 2008 betrafen zahlreiche Beschwerden die Übermittlung von Daten an Dritte ohne Einwilligung des Betroffenen.

Auffällig war insbesondere auch die Anzahl der Beschwerden wegen unerwünschter oder jedenfalls nicht erbetener Werbung per Post, E-Mail oder Telefon. Die Beschwerdeführer bemängelten nicht nur, dass sie diese Werbung unerwünscht erhalten hätten, sondern begehrten darüber hinaus weiterhin auch häufig Auskunft über die Herkunft der Daten und deren Verwendungszweck. Zudem wurde zumeist auch eine Löschung oder Sperrung der Daten und eine Bestätigung dieser Vorgänge gefordert, eine Untersagung der zukünftigen Speicherung ohne Genehmigung sowie der Übermittlung an Dritte ausgesprochen bzw. die Löschung aller gespeicherten Daten beantragt. Häufig schien dies den Beschwerdeführern ohne Einschaltung des Beauftragten für den Datenschutz bei der Landeszentrale in einer für sie akzeptablen Zeit nicht möglich zu sein.

Einige Fälle waren wieder auf eine Verwechslung von Daten bei Anbietern zurückzuführen. In anderen Fällen musste die Zulässigkeit des vorliegenden Handels mit Adressen zu Werbezwecken geprüft werden. Die einschlägigen Vorschriften hierzu wurden durch die BDSG-Novelle II vom 14.08.2009⁶⁷ erheblich verändert.

Neben der Bearbeitung der Anfragen der Beschwerdeführer mussten auch grundsätzliche datenschutzrechtliche Fragestellungen untersucht werden. So stellte sich u.a. die Frage nach der grundsätzlichen Zulässigkeit von Webcams im Internet. Da die für die Beurteilung dieser Rechtsfrage maßgeblichen Überlegungen einerseits sehr allgemeiner Natur sind und deren Beantwortung andererseits Folgewirkungen für sehr viele ähnliche Angebote haben könnte, schien eine Abstimmung mit den anderen bayerischen Datenschutzaufsichtsinstitutionen und die Entwicklung einer einheitlichen Einschätzung als ratsam, wenn nicht gar notwendig. Im Kern dieser Überlegungen stand die Frage, unter welchen Voraussetzungen angenommen werden kann, dass bei solchen in der Regel frei zugänglichen Angeboten im Internet personenbezogene Daten anfallen. Diese Frage steht letztlich auch im Zentrum der datenschutzrechtlichen Diskussion um das Angebot „Google Streetview“ und wird in diesem Zusammenhang auch weiterhin intensiv diskutiert.

Eine andere grundlegende datenschutzrechtliche Frage war, ob, wann und unter welchen Voraussetzungen der Abschluss eines Vertrages über die Nutzung von Rundfunkangeboten mit der Einwilligung in eine Datennutzung verbunden werden kann, und somit der betreffende Vertrag nur dann zustande kommt, wenn der Betroffene in die Nutzung seiner Daten einwilligt. Die in diesem Zusammenhang maßgeblichen Vorschriften waren zunächst noch im TMG enthalten, wurden aber mit den Datenschutznovellen des Jahres 2009 inhaltlich verändert und befinden sich nun im BDSG bzw. TKG⁶⁸. Entscheidend ist hierbei neben der Frage, ob eine solche Koppelung überhaupt zulässig ist, wie

⁶⁷ Vgl. oben 2.2.1.2.

⁶⁸ Vgl. oben 2.2.1.2. und 2.2.3.

die Einwilligungserklärung ausgestaltet sein muss, um Wirksamkeit erlangen zu können.

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

6. Weiterbildung

Die kontinuierliche Weiterbildung beruhte auf dem laufenden Studium periodisch erscheinender Fachliteratur, dem Besuch von Fortbildungs- und Fachveranstaltungen zu den verschiedensten Aspekten des Datenschutzes und dem Kontakt zu anderen Datenschutzinstitutionen. Zudem besuchte ich auch im Berichtszeitraum regelmäßig die Sitzungen und Veranstaltungen der Gesellschaft für Datenschutz und Datensicherheit e.V. und hierbei insbesondere die Sitzungen des Erfa-Kreises Bayern, in denen einerseits ausgewählte Institutionen und Firmen in Vorträgen und Erfahrungsberichten ihre besonderen Aufgabenschwerpunkte und die dabei zu beachtenden und zu bewältigenden datenschutzrechtlichen Herausforderungen vor- und zur Diskussion stellen. Andererseits werden in diesen Veranstaltungen auch allgemeine und spezielle datenschutzrechtliche Fragestellungen erörtert und von fachkundiger Seite über die aktuelle Rechtsentwicklung berichtet und diese fachlich bewertet.

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.