

Bayerische Landeszentrale für neue Medien

Achter Tätigkeitsbericht
des Beauftragten für den Datenschutz
bei der Bayerischen Landeszentrale für neue Medien
(Berichtszeitraum: 01.01.2006 bis 31.12.2007)

1. Vorbemerkung
2. Entwicklung des Datenschutzrechts
 - 2.1. Europäisches Recht
 - 2.1.1. Richtlinie zur Vorratsdatenspeicherung (2006/24/EG)
 - 2.1.2. Klage der EU- Kommission gegen die Bundesrepublik Deutschland wegen mangelnder Unabhängigkeit der Datenschutz-Kontrollstellen
 - 2.2. Bundesrecht
 - 2.2.1. Bundesdatenschutzgesetz (BDSG)
 - 2.2.2. Telekommunikationsgesetz (TKG)
 - 2.2.3. Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG
 - 2.2.4. Beschluss des Bundesverfassungsgerichts vom 23. Februar 2007 zur Videoüberwachung öffentlicher Plätze
 - 2.2.5. Entscheidung des Bundesgerichtshofs zu verdeckten Online-Durchsuchungen vom 31. Januar 2007
 - 2.2.6. Telemediengesetz (TMG)
 - 2.2.7. Allgemeines Gleichbehandlungsgesetz (AGG)
 - 2.2.8. Informationsfreiheitsgesetz des Bundes (IFG)
 - 2.2.9. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität

- 2.3. Bayerisches Landesrecht
 - 2.3.1. Rundstaatsvertrag (RStV)
 - 2.3.2. Bayerisches Mediengesetz (BayMG)
 - 2.3.3. Gesetz zur Ausführung des Rundfunkstaatsvertrags und des Jugendmedienschutzstaatsvertrags
- 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
 - 4.4. Umgang mit personenbezogenen Daten
 - 4.5. Auskunftersuchen, Anfragen, Beschwerden
 - 4.6. Datensicherheit
- 5. Datenschutz bei den Anbietern und Tochtergesellschaften der Landeszentrale
- 6. Weiterbildung
- 7. Schlussbemerkung

1. Vorbemerkung

Gemäß Art. 20 Abs. 6 Satz 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 achte Tätigkeitsbericht seit In-Kraft-Treten des BayMG am 01.12.1992 und bezieht sich auf die Jahre 2006 und 2007.

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

Förmliche Beanstandungen musste ich im Berichtszeitraum jedoch nicht aussprechen.

2. Entwicklung des Datenschutzrechts

2.1. Europäisches Recht

Das nationale Datenschutzrecht ist zunehmend durch Vorgaben der Europäischen Union vorgeprägt. 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. Richtlinie zur Vorratsdatenspeicherung (2006/24/EG)

Nach intensiven Diskussionen sowohl auf europäischer als auch auf deutscher Ebene wurde am 15.03.2006 die Richtlinie zur Vorratsdatenspeicherung 2006/24/EG² erlassen. Diese Richtlinie fordert Speicherpflichten für alle Anbieter öffentlicher elektronischer Kommunikationsdienste und öffentlicher Kommunikationsnetze und betrifft somit alle Dienste, die über Fest- oder Mobilfunknetze erbracht werden, wie etwa Telefon, Fax, SMS, MMS, E-Mail,

¹ Richtlinie 95/46/EG, ABl. EG v. 23.11.1995, Nr. L 281/31.

² Richtlinie über die Vorratsspeicherung 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, ABl. EG v. 15.03.2006, Nr. L 105/54.

Filetransfer, www, Chat- und Newsgroups. Von jeder Kommunikationsverbindung sind die Daten zu speichern, die erforderlich sind, um Sender und Empfänger zu identifizieren, um Datum, Zeit und Dauer der Kommunikation festzuhalten, um die Kommunikationsausrüstung der Nutzer, die benutzten Dienste und bei mobiler Kommunikation auch die Funkzelle festzuhalten, aus der die Kommunikation geführt wurde. Auch die Daten von Verbindungsversuchen sind zu speichern, sofern solche Daten beim Anbieter entstanden sind.

Diese Daten sind für mindestens sechs und höchstens 24 Monate zu speichern, um den zuständigen staatlichen Behörden den Zugriff auf diese Daten zu ermöglichen, wenn diese mit dem Ziel tätig sind, „schwere Verbrechen“ zu verhüten, zu untersuchen, aufzuklären und zu verfolgen. Für die Umsetzung dieser Richtlinie wurde den nationalen Gesetzgebern eine Frist bis spätestens 15.09.2007 eingeräumt; bis dahin mussten die diese Richtlinie umsetzenden nationalen Vorschriften Rechtskraft erlangt haben.³

Der Inhalt dieser Richtlinie war im Vorfeld auf verschiedenen Ebenen kontrovers diskutiert worden. Widerstände existierten einerseits von Seiten der zu verpflichtenden Kommunikationsanbieter, die die Vorratsdatenspeicherung durchführen sollen, ohne dafür einen Kostenersatz, zu erhalten. Andererseits wurde der Inhalt dieser Richtlinie auch von Datenschützern kritisch kommentiert, da diese Dateien ohne konkreten Anlass ausschließlich für den Fall gespeichert werden sollen, dass sich zu einem späteren Zeitpunkt ein hinreichender Anlass für die Speicherung dieser Daten ergeben sollte. Zweifel wurden auch hinsichtlich der Ermächtigungsgrundlage der Europäischen Union geäußert. Die Beschlussfassung im Rat der Europäischen Union war gegen die Stimmen der Slowakei und Dänemarks erfolgt. Die Mitgliedsstaaten Irland und Slowakei hatten beim EuGH Klage gegen diese Richtlinie erhoben, weil diese Richtlinie keine hinreichende Rechtsgrundlage habe.⁴

³ Für die Vorratsdatenspeicherung von Internetdaten besteht die Möglichkeit, die Umsetzung um bis zu 36 Monaten aufzuschieben, vgl. Art. 13 Abs. 3 der Richtlinie. Die Bundesregierung hatte sich dieses Recht vorbehalten.

⁴ Der EuGH hat die Klage unterdessen mit Urteil vom 10. Februar 2009 abgewiesen. Die Begründung lässt sich dahingehend zusammenfassen, dass sich die Richtlinie auf Art. 95 EG stützen könne, da sich ihre Bestimmungen (einschließlich der Speicherverpflichtungen) im Wesentlichen auf die Tätigkeiten der Diensteanbieter beschränke, den Zugang zu den Daten bzw. die Nutzung durch die Mitgliedstaaten nicht regle und daher die Richtlinie in überwiegenderem Maße das Funktionieren des Binnenmarktes betreffe. Diese Begründung erscheint vor allem deshalb diskussionswürdig, weil die Richtlinie keineswegs nur Speicherverpflichtungen 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 der jeweilige nationale Gesetzgeber eine solche Verpflichtung einführen könnte oder würde. Ebenso erscheint zweifelhaft, ob eine solche Verpflichtung wirklich für das Funktionieren des Binnenmarktes erforderlich ist.

Zwar beantragte auch die Opposition im Bundestag, gegen die Richtlinie vor dem EuGH zu klagen, konnte sich aber mit diesem Antrag nicht gegen die Regierungsfractionen durchsetzen.

In Deutschland wurde die Richtlinie mit dem „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/ EG“⁵ umgesetzt. Das Gesetz wurde am 09.11.2007 im Bundestag verabschiedet und am 26.12.2007 von Bundespräsident Köhler unterzeichnet. Es trat am 01.01.2008 in Kraft.

2.1.2. Klage der EU- Kommission gegen die Bundesrepublik Deutschland wegen mangelnder Unabhängigkeit der Datenschutz-Kontrollstellen

Nachdem die Europäische Kommission am 05.07.2005 ein Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland eingeleitet hatte, ist in diesem Fall nach gescheiterten Einigungsversuchen seit dem 22. November 2007 ein Klageverfahren vor dem EuGH anhängig. Die Kommission monierte zuvor, dass die Datenschutzaufsicht über die Privatwirtschaft, so wie sie derzeit organisiert sei, nicht über die von der EU-Datenschutzrichtlinie⁶ 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 Anforderungen der Richtlinie im Hinblick auf die Unabhängigkeit dieser Kontrollstellen entsprächen.

Für die Datenschutzaufsicht über den nicht-öffentlichen Bereich ist in Bayern zentral die Regierung von Mittelfranken zuständig, die als staatliche Mittelbehörde sicherlich keine völlige Unabhängigkeit von den übrigen staatlichen Institutionen des Freistaates Bayern und insbesondere vom Staatsministerium des Innern besitzt. Dies ist aber gerade die Forderung, die die Europäische Kommission im Hinblick auf Art. 28 Abs. 1 der EU-Datenschutzrichtlinie

⁵ BGBl 2008, I, S. 70

⁶ Richtlinie 95/46/EG, ABl. EG v. 23.11.1995, Nr. L 281, S. 31.

erhebt. Die Staatsregierung hat zwar mit Beschluss vom 03.02.2009 beschlossen, die in der Regierung von Mittelfranken angesiedelte Datenschutzaufsicht zum „Landesamt für Datenschutzaufsicht“ auszubauen. Dass dieses Landesamt jedoch eine völlige Unabhängigkeit in dem oben genannten Sinne von anderen staatlichen Institutionen erhalten soll, erscheint jedoch unwahrscheinlich, auch wenn nähere Details noch nicht bekannt sind. Unmöglich wäre es indes nicht.

Im Gegensatz dazu vertritt die Bundesrepublik Deutschland in diesem Verfahren offenbar die Auffassung⁷, 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 den jeweiligen Mitgliedsstaaten unberührt lasse.

Mit der Klage verfolgt die Europäische Kommission die Absicht, die Bundesrepublik Deutschland doch noch zur Einführung einer in dem oben genannten Sinne unabhängigen Datenschutzaufsicht zu bewegen.

Für den Bereich der Landeszentrale bestehen derartige Zweifel an der Unabhängigkeit des Beauftragten für den Datenschutz nicht; dieser ist nach Art. 20 Abs. 3 Satz 6 BayMG in der Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen⁸. Da auch die gelebte Praxis bei der Landeszentrale diesen Vorgaben entspricht, dürften diese Verhältnisse auch den Vorstellungen der Europäischen Kommission im Hinblick auf Art. 28 Abs. 1 der EU-Datenschutzrichtlinie entsprechen, so dass für den Bereich der Landeszentrale wie auch ihrer Anbieter sicherlich richtlinienkonforme Bedingungen bestehen.

2.2. Bundesrecht

2.2.1. Bundesdatenschutzgesetz (BDSG)

Das Bundesdatenschutzgesetz wurde am 26.08.2006 durch das „Erste Gesetz zum Abbau bürokratischer Hemmnisse insbesondere der mittelständischen Wirtschaft“⁹ geändert. Die Änderungen betreffen ausschließlich den nicht-öffentlichen Bereich.

⁷ Vgl. die Mitteilung über die Klageeinreichung im Amtsblatt der Europäischen Union vom 09.02.2008 zur Rechtssache C-518/07.

⁸ Vgl. dazu unten die Ausführungen zur Funktion des Beauftragten für den Datenschutz unter 3.

⁹ BGBl. I 2006, S. 1970

Grundsätzlich müssen weiterhin alle Stellen im nicht-öffentlichen Bereich, die personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung (z.B. Adresshandel, Auskunfteien, etc) oder zum Zweck der anonymisierten Übermittlung (z.B. Markt- und Meinungsforschung) automatisiert verarbeiten, unabhängig von der Anzahl der Beschäftigten einen betrieblichen Datenschutzbeauftragten bestellen (§ 4f Abs. 1 S.1 und 6 BDSG). Dies gilt auch, wenn die automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, die eine Vorabkontrolle erfordern (§ 4d Abs. 5 BDSG).

In den übrigen Fällen müssen nicht-öffentliche Stellen erst dann einen Datenschutzbeauftragten bestellen, wenn mehr als neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind (§ 4f Abs. 1 S. 4 BDSG). Damit wurde die Mindestanzahl der Beschäftigten von bisher mehr als vier auf mehr als neun heraufgesetzt.

Werden die personenbezogenen Daten nicht automatisiert, sondern in anderer Weise erhoben, verarbeitet oder genutzt, so ist es dabei geblieben, dass ein Datenschutzbeauftragter erst bestellt werden muss, wenn mindestens zwanzig Personen damit beschäftigt sind (§ 4f Abs. 1 S. 3 BDSG).

Trifft das nicht-öffentliche Unternehmen nach diesen Regeln keine Verpflichtung, einen betrieblichen Datenschutzbeauftragten zu benennen, so muss gemäß § 4g Abs. 2a BDSG nun der Leiter der nicht-öffentlichen Stelle in anderer Weise sicherstellen, dass die gesetzlichen Aufgaben eines betrieblichen Datenschutzbeauftragten erfüllt werden.

Die Aufsichtsbehörden sind nun auch zur Beratung der betrieblichen Datenschutzbeauftragten verpflichtet (§ 38 Abs. 1 BDSG). Dies stellt für den Datenschutzbeauftragten der Landeszentrale keine Neuerung dar, da diese Beratung bereits bisher gemäß Art. 20 Abs. 3 BayMG durchgeführt wurde.

Gegenwärtig wird ein Gesetzentwurf der Bundesregierung¹⁰ beraten, der neben Fragen zum Datenschutzaudit auch die Änderungen des BDSG enthält, die die Lehren aus einigen Datenschutzskandalen des vergangenen Jahres ziehen sollen, die seinerzeit in einem Datenschutzgipfel

¹⁰ Die Bundesregierung hat am 10.12.2008 den vom Bundesinnenministerium erarbeiteten Gesetzentwurf angenommen und an den Bundesrat weitergeleitet, vgl. BR-Drs. 4/09).

politisch vereinbart wurden. Dabei sollen die Rechte der Betroffenen insbesondere hinsichtlich der Weitergabe ihrer Daten zu Werbezwecken in Listenform gestärkt werden, die nach dem bisherigen Recht noch weitgehend auch ohne Einwilligung der Betroffenen möglich ist. Künftig soll der hierfür entscheidende § 28 BDSG dahingehend geändert werden, dass im Wesentlichen nur noch eine Nutzung bestimmter Daten für eigenen Werbe- bzw. Marktforschungszwecke ohne entsprechende Einwilligung zulässig sein wird. Darüber hinaus soll die Einwilligung des Betroffenen erforderlich sein, die diesem zumindest schriftlich bestätigt oder bei einer elektronischen Erklärung protokolliert und zum jederzeitigen Abzuruf und möglichen Widerruf vorgehalten werden muss.

2.2.2. Telekommunikationsgesetz (TKG)

Zum Zwecke der Umsetzung der Vorgaben des europäischen TK-Richtlinienpaketes war das Telekommunikationsgesetz (TKG) einer umfassenden Novellierung unterzogen worden. Hierüber war im letzten Tätigkeitsbericht ausführlich berichtet worden. Das neue TKG¹¹ ist am 26.06.2004 in Kraft getreten und enthielt erstmals einen eigenen abschließenden Datenschutzteil (§§ 91 – 107 TKG) und somit eine umfassende gesetzliche Regelung für den Datenschutz in der Telekommunikation. Die parallel geltende Telekommunikations-Datenschutzverordnung war damit überflüssig geworden und konnte entfallen.

Nach dem neuen TKG war erstmals die sog. Inverssuche unter bestimmten Umständen zulässig geworden, bei der die Telefonauskunft den zu einer Telefonnummer gehörenden Namen und die Anschrift des Teilnehmers bekannt gibt, § 105 Abs. 2 Satz 2 TKG. Datenschutzrechtlich bedeutsam war auch, dass Anbieter von Prepaid-Produkten, nachdem das Bundesverwaltungsgericht am 22.10.2003 noch entschieden hatte, dass eine Verpflichtung zur Speicherung des Namens und der Adresse des Kunden nicht bestehe, durch die Neufassung des § 111 Abs. 1 Satz 1 TKG verpflichtet wurden, Daten über den Namen, die Anschrift und das Geburtsdatum des Rufnummerninhabers zu erheben und zu speichern, auch wenn diese Daten für betriebliche Zwecke des Anbieters nicht erforderlich sind.

¹¹ Vgl. BGBl. 2004 I S. 1190

Zur Erfüllung ihrer gesetzlichen Aufgaben haben eine Vielzahl von Stellen die Möglichkeit auf diese Bestandsdaten zurück zu greifen (§ 112 Abs. 2 TKG). Hierzu zählen Gerichte, Strafverfolgungsbehörden, Polizeivollzugsbehörden des Bundes und der Länder für Zwecke der Gefahrenabwehr, Zollkriminalamt und Zollfahndungsämter für Zwecke eines Strafverfahrens, Zollkriminalamt zur Vorbereitung und Durchführung von Maßnahmen nach § 39 des Außenwirtschaftsgesetzes, Verfassungsschutzbehörden des Bundes und der Länder, Militärischer Abschirmdienst, Bundesnachrichtendienst, Notrufabfragestellen, Bundesanstalt für Finanzdienstleistungsaufsicht, Zollverwaltung zur Schwarzarbeitsbekämpfung.

Über diese Vorgaben hinaus sind Anbieter von Telekommunikationsdiensten auch verpflichtet, individuelle Auskünfte über Bestandsdaten zu erteilen (§ 113 TKG). Diese Regelung erlaubt es beispielsweise, bei einem Internetzugangsanbieter zu erfragen, welchem Kunden eine dynamisch vergebene IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war. Abgefragt werden können auch Passwörter, PINs und PUKs. Auskunft ist den Stellen zu erteilen, die für die Verfolgung von Straftaten und Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung und für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes zuständig sind. Hierzu würde daher auch die Landeszentrale gehören, soweit sie zur Verfolgung von Ordnungswidrigkeiten zuständig ist. Bisher war ein solches Auskunftersuchen allerdings noch nie erforderlich und wurde daher auch nicht gestellt.

2.2.3. Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG

Zur Umsetzung der Vorgaben der oben genannten Richtlinie 2006/24/ EG zur Vorratsdatenspeicherung war eine durchgreifende Änderung des Telekommunikationsrechts erforderlich geworden. Zu diesem Zwecke wurde das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG¹² beschlossen, das am 01. Januar 2008 in Kraft trat.

¹² Vgl. BGBl. 2007 I, S. 3198.

Nach dem mit diesem Gesetz eingeführten § 113a TKG ist derjenige, der öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, verpflichtet, die folgenden Daten sechs Monate zu speichern:

- Anbieter von Telefondiensten einschließlich Mobilfunk- und Internet-Telefondiensten speichern
 - die Rufnummer oder andere Kennung des anrufenden und des angerufenen Anschlusses sowie im Falle von Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses
 - den Beginn und das Ende der Verbindung nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone
 - in Fällen, in denen im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können, Angaben zu dem genutzten Dienst.
- Bei mobilen Telefondiensten werden zudem gespeichert:
 - die internationale Kennung für mobile Teilnehmer für den anrufenden und den angerufenen Anschluss
 - die internationale Kennung des anrufenden und des angerufenen Endgerätes
 - die Bezeichnung der durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzten Funkzellen.
- Bei im Voraus bezahlten anonymen Diensten wird auch die erste Aktivierung des Dienstes nach Datum, Uhrzeit und Bezeichnung der Funkzelle, bei Internet-Telefondiensten auch die Internetprotokoll-Adresse des anrufenden und des angerufenen Anschlusses gespeichert.

Das gilt entsprechend bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht; hierbei sind zudem die Zeitpunkte der Versendung und des Empfangs der Nachricht zu speichern.
- Anbieter von Diensten der elektronischen Post (E-Mail) speichern
 - bei Versendung einer Nachricht die Kennung des elektronischen Postfachs und die Internetprotokoll-Adresse des Absenders sowie die Kennung des elektronischen Postfachs jedes Empfängers der Nachricht,
 - bei Eingang einer Nachricht in einem elektronischen Postfach die Kennung des elektronischen Postfachs des Absenders und des Empfängers der Nachricht sowie die Internetprotokoll-Adresse der absendenden Telekommunikationsanlage,

- bei Zugriff auf das elektronische Postfach dessen Kennung und die Internetprotokoll-Adresse des Abrufenden,
 - zudem die Zeitpunkte der Nutzungen der Dienste nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone.

- Anbieter von Internetzugangsdiensten speichern
 - die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse
 - eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt
 - den Beginn und das Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone.

Wer Telekommunikationsdienste erbringt und hierbei die nach Maßgabe dieser Vorschrift zu speichernden Angaben verändert, ist zur Speicherung der ursprünglichen und der neuen Angabe sowie des Zeitpunktes der Umschreibung dieser Angaben nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone verpflichtet.

Anbieter von Mobilfunknetzen für die Öffentlichkeit haben zu den Bezeichnungen der Funkzellen auch die Daten zu speichern, aus denen sich die geografische Lage der jeweiligen Funkzelle sowie die Hauptstrahlrichtung der Funkantenne ergibt.

Der Gesetzestext nimmt auch Privatpersonen von der Pflicht zur Speicherung nicht aus, etwa wenn sie kostenlos einen öffentlichen WLAN-Zugang oder einen E-Mail-Dienst anbieten. Dagegen sind Anbieter von Webseiten, Webspace (Hosting), Foren und Chat-Diensten nicht betroffen. Anbieter von Internetzugängen, Internet-Telefonie und E-Mail sind erst ab dem 1. Januar 2009 zur Speicherung verpflichtet; mehrere Provider haben angekündigt, diese Übergangsfrist wahrzunehmen.

Genutzt und übermittelt werden dürfen die auf Vorrat gespeicherten Verbindungsdaten nach § 113b TKG nur

- zur Verfolgung von Straftaten,
- zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit,
- zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes an die zuständigen Stellen, aber auch
- zur Erteilung von Auskünften über die Identität von Telekommunikationsnutzern nach § 113 TKG.

Eine eigene Abrufbefugnis enthält allerdings auch § 113b TKG nicht, sondern setzt vielmehr eine gesonderte gesetzliche Bestimmung über den Datenabruf unter Bezugnahme auf § 113a TKG voraus. Bislang ist eine solche lediglich in § 100g StPO vorgesehen. Ein Zugriff auf die Vorratsdaten ist danach möglich bei der Verfolgung von Straftaten von auch im Einzelfall erheblicher Bedeutung, darüber hinaus aber auch wenn bestimmte Tatsachen den Verdacht begründen, dass eine Straftat mittels Telekommunikation begangen wurde.

Private Rechteinhaber haben daher über § 100g StPO keinen direkten Zugriff auf die auf Vorrat gespeicherten Daten. Sie könnten aber Strafanzeige erstatten und dann ggf. die Ermittlungsakten einsehen, was zum gleichen Ergebnis führen kann.

Ausgeweitet wurde zudem auch die oben unter 2.2.2 bereits angesprochene Identifizierungspflicht nach § 111 Abs. 1 TKG auf alle Nutzungen mit dauerhafter Anschlusskennung. Darunter fallen etwa Telefonanschlüsse, Handykarten und DSL-Anschlüsse. E-Mail-Anbieter sind von der Identifizierungspflicht ausgenommen. Sofern sie Daten über die Identität ihrer Nutzer erheben, müssen sie diese Angaben für Zwecke der Auskunftserteilung an Behörden auch speichern.

Die Anbieter der von der Identifizierungspflicht betroffenen Dienste haben nunmehr vor der Freischaltung des Nutzers folgende Daten in Dateien zu speichern, die zum jederzeitigen Abruf durch die Bundesnetzagentur bereit zu halten sind. Dies sind:

- die vergebene Rufnummer bzw. E-Mail-Adresse,
- Name und Anschrift des Inhabers,
- das Datum des Vertragsbeginns,
- das Geburtsdatum des Inhabers,
- bei Festnetzanschlüssen auch die Anschrift des Anschlusses.

Gelöscht werden die Daten am Ende des auf das Vertragsende folgenden Jahres (§ 111 Abs. 4 TKG).

Gegen dieses Gesetz wurde von verschiedenen Seiten Verfassungsbeschwerde erhoben. Auf einen Eilantrag hin schränkte das Bundesverfassungsgericht in einer einstweiligen Anordnung am 11. März 2008¹³ die Verwendungsmöglichkeit der auf Vorrat gespeicherten Daten stark ein. Die Verpflichtung zur Speicherung für die betroffenen Telekommunikationsunternehmen wurde jedoch nicht ausgesetzt. Das Bundesverfassungsgericht hat in diesem Beschluss festgestellt, dass in dem Abruf der Daten selbst eine schwerwiegender und nicht mehr rückgängig zu machender Eingriff in das Grundrecht aus Art 10 Abs. 1 GG liegt, weil ein solcher Abruf es ermöglicht, weitreichende Erkenntnisse über das Kommunikationsverhalten des Betroffenen und seine sozialen Kontakte zu erlangen. Daher sei die Verwendung der Daten durch Ermittlungsbehörden nur noch im Zusammenhang mit entsprechend schweren Straftaten zulässig. Eine endgültige Entscheidung im Hauptsacheverfahren ist noch nicht ergangen.

2.2.4. Beschluss des Bundesverfassungsgerichts zur Videoüberwachung öffentlicher Plätze

Nach dem Beschluss des Bundesverfassungsgericht vom 23.02.2007¹⁴ kann die Videoüberwachung öffentlicher Plätze, auch wenn sie der Sicherung eines Kunstwerkes auf einem städtischen Platz dient, nicht auf Art. 16 Abs. 1 bzw. Art. 17 Abs. 1 BayDSG gestützt werden.

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 stehen und den Eingriff nicht durch ihr Verhalten veranlasst haben.

Eine für einen solchen Eingriff hinreichende Ermächtigungsgrundlage muss Anlass, Zweck und Grenzen des Eingriffs bereichsspezifisch, präzise und normenklar festlegen. Dem genügen Art. 16 und 17 BayDSG nicht, da sie insoweit lediglich an die Zuständigkeit der handelnden Behörde anknüpfen und auf das dazu Erforderliche verweisen. Dies reicht

¹³ Beschluss vom 11.03.2008, 1 BvR 256/08, MMR 2008, S. 303 ff.

¹⁴ Beschluss der 1. Kammer des Ersten Senats des Bundesverfassungsgerichtes vom 23. Februar 2007, 1 BvR 2368/06.

zur Rechtfertigung der mit der Videoüberwachung verbundenen, schwer wiegenden Grundrechtseingriffe nicht aus. Solche Eingriffe könnten nur dann gerechtfertigt werden, wenn für die Videoüberwachung ein hinreichender Anlass besteht und das Übermaßverbot in räumlicher und zeitlicher Hinsicht, auch gerade im Hinblick auf die Aufzeichnung und Auswertung der Bilder gewahrt bleibe.

Diese Entscheidung ist auf Aufnahmen von Rundfunkveranstaltern zwar nicht unmittelbar übertragbar, da die mit solchen Aufnahmen verfolgten Zwecke in der Regel völlig andere als die im Fall der Entscheidung des Bundesverfassungsgerichtes sind. Gleichwohl benennt die Entscheidung die dabei zu berücksichtigenden privaten Belange der hierbei ggf. auch unbeabsichtigt aufgenommenen aber gleichwohl betroffenen Personen. Zu berücksichtigen ist in diesem Zusammenhang, dass der Eingriff in die angesprochenen Grundrechte auch nicht dadurch entfällt, dass lediglich Verhaltensweisen im öffentlichen Raum aufgenommen werden. Das allgemeine Persönlichkeitsrecht gewährleistet nicht allein den Schutz der Privat- und Intimsphäre, sondern trägt nach ständiger Rechtsprechung des Bundesverfassungsgerichtes in der Gestalt des Rechts auf informationelle Selbstbestimmung auch den informationellen Schutzinteressen des Einzelnen, der sich in die Öffentlichkeit begibt, Rechnung. Diese Frage spielte in der Beratungstätigkeit gegenüber den Anbietern im Berichtszeitraum eine gewisse Rolle.

2.2.5. Entscheidung des Bundesgerichtshofs (BGH) zu verdeckten Online-Durchsuchungen vom 31. Januar 2007

Nach dem Beschluss des BGH vom 31.01.2007¹⁵ war es den Ermittlungsbehörden nach der Strafprozessordnung (StPO) nicht erlaubt, den Computer eines Beschuldigten und die dort gespeicherten Dateien mit Hilfe eines Programms, das ohne Wissen des Betroffenen aufgespielt wurde (verdeckte Online-Durchsuchung), heimliche zu durchsuchen. Der BGH stellt in dieser Entscheidung klar, dass das Bild der StPO von einer rechtmäßigen Durchsuchung dadurch geprägt ist, dass Ermittlungsbeamte am Ort der Durchsuchung anwesend sind und dass die Ermittlung offen gelegt wird.

Durch eine Reihe von Vorgaben zur Durchführung soll sichergestellt werden, dass der Betroffene jedenfalls unmittelbar nach Beendigung der Maßnahme von der Durchsuchung und über ihren Grund informiert wird

¹⁵ Beschluss vom 31. Januar 2007 - StB 18/06

und damit Gelegenheit erhält, deren Rechtmäßigkeit überprüfen zu lassen. Die diesbezüglichen Vorgaben zur Durchführung der Durchsuchung sind daher nach ihrem Sinn und Zweck, den von der Durchsuchung betroffenen zu schützen, als wesentliche Förmlichkeiten zwingendes Recht und nicht lediglich Vorschriften, die zur ermittlungstaktischen Disposition stehen. Die beantragte verdeckte Online-Durchsuchung war daher als unzulässig abgelehnt worden.

2.2.6. Telemediengesetz (TMG)

Am 18.01.2007 wurde vom Bundestag das Gesetz zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz – ELGVG) beschlossen, das in Art. 1 das neu geschaffene Telemediengesetz (TMG) enthält. Der Bundesrat stimmte dem Gesetz am 16.02.2007 zu, so dass es am 01.03.2007 in Kraft treten konnte¹⁶.

Hintergrund des neuen Gesetzes sind die, auch im letzten Datenschutzbericht erwähnten, langjährigen Bestrebungen, einheitliche Regelungen für die elektronischen Medien zu schaffen, was für den Bereich des Jugendschutzes mit der Einführung des Jugendmedienschutz-Staatsvertrages¹⁷ bereits früher geglückt war. Diesem Vorbild folgend wurde nun die sprachliche Unterscheidung zwischen Telediensten und Mediendiensten aufgehoben und beide Dienste unter dem einheitlichen Begriff der „Telemedien“ zusammengefasst. Einer Verabredung zwischen Bund und Ländern folgend sind nun im Telemediengesetz die wirtschaftsbezogenen Bestimmungen für Telemedien enthalten, während die darüber hinausgehenden inhaltespezifischen Regelungen im Rundfunkstaatsvertrag vorgegeben werden (vgl. hierzu unten 2.3.1).

Diese Neuregelung gewährleistet, dass die Rahmenbedingungen für den elektronischen Geschäftsverkehr mit Blick auf die wirtschaftliche Entwicklung der neuen elektronischen Dienste auch zukünftig unabhängig vom Verbreitungsweg entwicklungssoffen ausgestaltet werden. Dabei sind die inhaltlichen Anforderungen, abgesehen von den erforderlichen redaktionellen Änderungen, weitestgehend unverändert geblieben. Dies gilt insbesondere auch für den Datenschutz, der künftig im IV. Abschnitt

¹⁶ BGBl. I 2007, S. 179, 251

¹⁷ Staatsvertrag über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien (Jugendmedienschutz-Staatsvertrag – JMStV) vom 10./27. September 2002, BayGVBl 2003 S. 147.

des Telemediengesetzes bereichsspezifisch geregelt ist. Grundsätzlich wurde dabei das im TDDSG und dem MDStV bestehende datenschutzrechtliche System übernommen.

Inhaltliche Neuerungen enthält das Telemediengesetz einerseits dahingehend, dass kommerzielle Kommunikation (die gelegentlich auch als Spam-Mail bezeichnet wird) per elektronischer Post seither nur noch dergestalt versandt werden darf, dass in der Kopf- und Betreffzeile weder der Absender noch der kommerzielle Charakter der Nachricht verschleiert oder verheimlicht werden darf. Andererseits soll, und dies ist datenschutzrechtlich von erheblicher Bedeutung, die Übermittlung von Bestands- wie auch Nutzungsdaten nicht nur zur Strafverfolgung und zur Erfüllung der Aufgaben von Geheimdiensten, sondern neuerdings auch insoweit zulässig sein, als dies zur Durchsetzung der Rechte am geistigen Eigentum erforderlich ist.

Im Prinzip wurde jedoch weitestgehend das aus dem alten Teledienstdatenschutzgesetz (TDG) bekannte System übernommen. So gelten die Vorschriften nicht für die Erhebung und Verwendung personenbezogener Daten der Nutzer, sofern es um die Nutzer solcher Dienste im Dienst- und Arbeitsverhältnis geht (§ 11 Abs. 1 Satz 1 Nr. 1 TMG). Die Bestimmungen gelten ebenso wenig für die Erhebung und Verwendung personenbezogener Daten innerhalb von oder zwischen nicht öffentlichen Stellen oder öffentlichen Stelle, sofern dies ausschließlich zur Steuerung von Arbeits- und Geschäftsprozessen erfolgt (§ 11 Abs. 1 Satz 1 Nr. 2 TMG).

Die Verwendung personenbezogener Daten bleibt weiterhin grundsätzlich verboten, es sei denn, es liegt eine Einwilligung des Nutzers oder eine gesetzliche Ermächtigung vor. Die gesetzliche Ermächtigung muss sich aber entweder aus dem TMG oder einer anderen Regelung ergeben, die sich ausdrücklich auf Telemedien bezieht (§ 12 TMG).

Hinsichtlich der Einwilligung des Nutzers ist zu beachten, dass diese gemäß § 13 Abs. 2 TMG auch auf elektronischem Wege erklärt werden kann. Da eine wirksame elektronische Einwilligung jedoch an zahlreiche Voraussetzungen geknüpft ist (so muss der Diensteanbieter sicherstellen, dass der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat, die Einwilligung protokolliert wird, der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und der Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann), hat diese soweit erkennbar zumindest im Berichtszeitraum noch keine weite Verbreitung gefunden.

Gewisse Schwierigkeiten bietet weiterhin die Abgrenzung zum Bundesdatenschutzgesetz, auch wenn in § 11 Abs. 2 TMG klar gestellt wurde, dass der Nutzer und damit datenschutzrechtliche Adressat nur eine natürliche Person sein kann.

In § 14 Abs. 2 TMG ist ein Auskunftsanspruch gegen Diensteanbieter und somit auch gegen Online-Provider vorgesehen. Neben einer Auskunft über Bestandsdaten¹⁸ gegenüber Strafverfolgungs- und bestimmten staatlichen Sicherheitsbehörden ist eine solche auch zur Durchsetzung von Rechten am geistigen Eigentum grundsätzlich vorgesehen, so dass die aus der Telemediennutzung stammenden Bestandsdaten neben öffentlichen Zwecken auch für privatnützige Zielsetzungen prinzipiell zur Verfügung stehen.

Nutzungsdaten¹⁹ umfassen neben der Identifikation des Nutzers Daten über den Beginn, das Ende und den Umfang der Nutzung wie auch Angaben über die in Anspruch genommenen Telemedien, und können daher durchaus Rückschlüsse auf die Interessen und Ansichten des einzelnen Nutzers zulassen. Sogar Nutzungsprofile dürfen erstellt werden, allerdings nur unter Verwendung von Pseudonymen. In Anbetracht der Tatsache, dass es sich bei massenkommunikativen Telemedien in der Regel um Rundfunk im Sinne des Verfassungsrechtes handelt²⁰, eröffnet dies den Anbietern durchaus beachtliche und daher nicht immer unproblematische Möglichkeiten, zumal sogar die Weitergabe an Dritte zum Zwecke der Marktforschung zulässig ist²¹, diese allerdings nur in anonymisierter Form. Zudem sieht § 15 Abs. 3 Satz 3 TMG vor, dass die Nutzungsprofile nicht mit den Daten über die Träger des Pseudonyms zusammengebracht werden dürfen, und gewährleistet damit zumindest die unerlässlichen verfassungsrechtlichen Anforderungen des Rundfunkrechts.

Insbesondere im Hinblick auf die in § 15 Abs. 5 Satz 4 TMG angeordnete entsprechende Anwendung der in § 14 Abs. 2 TMG enthaltenen Auskunftsverpflichtungen bedürfen die verfassungsrechtlichen Grenzen einer

¹⁸ Bestandsdaten werden in § 14 Abs. 1 TMG als solche definiert, die für die Begründung, inhaltliche Ausgestaltung und Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind.

¹⁹ Nutzungsdaten definiert § 15 Abs. 1 TMG als solche, die erforderlich sind, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen.

²⁰ Zudem bilden die Regeln der §§ 11 bis 15 TMG durch die dynamische Verweisung in § 47 Abs. 1 RStV auch den wesentlichen datenschutzrechtlichen Ordnungsrahmen für die Nutzung von Rundfunkprogrammen im Sinne des Rundfunkstaatsvertrages.

²¹ Vgl. § 15 Abs. 5 Satz 3 TMG.

solchen Datenerfassung und -weitergabe einer besonderen Beobachtung. Dies gilt nochmals verstärkt für solche Daten, die sich auf die Nutzung von der Rundfunkfreiheit unterliegenden Angeboten beziehen. Da Strafverfolgungs- wie auch Sicherheitsbehörden, Nachrichtendienste und Rechteinhaber allenfalls am Rande Marktforschung betreiben und daher zumeist an pseudonymisierten Daten nicht interessiert sein dürften, wird für diese in aller Regel nur die Weitergabe von Nutzungsdaten und Nutzungsprofilen mit offenem Bezug zum Nutzer bedeutsam sein. Nutzungsprofile über das Konsumieren von Rundfunkprogrammen ist verfassungsrechtlich aber äußerst problematisch, so dass hier nur mit sehr großer Zurückhaltung und nach strenger Prüfung der in Rede stehenden Interessen, Schutzgüter und Grundrechtspositionen vorgegangen werden kann und darf.

2.2.7. Allgemeines Gleichbehandlungsgesetz (AGG)

Durch das Allgemeine Gleichbehandlungsgesetz²², das am 18. August 2006 in Kraft getreten ist, sollen Benachteiligungen von Bewerbern aus Gründen der Rasse, der Religion, des Geschlechts, einer Behinderung, des Alters usw. verhindert werden.

Das AGG erlangt seine datenschutzrechtliche Bedeutung dadurch, dass es sich bei den diskriminierungsrelevanten Daten grundsätzlich um besonders sensible personenbezogenen Daten i.S.v. § 3 Abs. 9 BDSG handelt.

Daher müssen datenschutzrechtliche Bedenken bei der Umsetzung des AGG berücksichtigt werden. Dies führt z.B. zu neutralen Stellenausschreibungen, veränderten Fragerechten, Anpassung von Personalbögen und die Berücksichtigung von Löschfristen für die Dokumentation.

Daneben müssen aber nun auch Bewerbungsunterlagen sowie Aufzeichnungen zum Bewerbungsverfahren aufbewahrt werden, wenn ein Bewerber nicht ausgewählt wurde. Das AGG sieht für den Fall der Diskriminierung in § 15 AGG einen Schadensersatzanspruch vor. Der Schadensersatzanspruch muss innerhalb von 2 Monaten nach Zugang der Ablehnungsmittel geltend gemacht werden. Er entsteht, wenn der abgelehnte Bewerber in einem nicht diskriminierenden Verfahren eingestellt worden wäre. Diese Umstände muss der betreffende Bewerber nachweisen, während der Arbeitgeber ggf. beweisen muss, dass keine Diskriminierung stattgefunden hat.

²² BGBl. I 2006, S. 1897, 1910

2.2.8. Informationsfreiheitsgesetz des Bundes (IFG)

Das Gesetz²³, das am 01. Januar 2006 in Kraft getreten ist, gewährt jedermann einen voraussetzungslosen Rechtsanspruch auf Zugang zu amtlichen Informationen von Bundesbehörden. Eine Begründung durch Interessen rechtlicher, wirtschaftlicher oder sonstiger Art ist nicht erforderlich.

„Amtliche Information“ ist dabei jede amtlichen Zwecken dienende Aufzeichnung, unabhängig von der Art ihrer Speicherung, also beispielsweise Schriftstücke in herkömmlichen Akten, elektronisch gespeicherte Informationen, Zeichnungen, Grafiken, Pläne, Ton- und Videoaufzeichnungen.

Der Anspruch richtet sich gegen Bundesbehörden im Sinne des Verwaltungsverfahrensgesetzes. Bedient sich eine Bundesbehörde zur Erfüllung ihrer Aufgaben einer juristischen oder natürlichen Person des Privatrechts, so ist sie auch dann auskunftspflichtig, wenn die begehrten Informationen bei der privatrechtlichen Person vorliegen.

Der Begriff der Informationsfreiheit ist jedoch mehrdeutig und deshalb potentiell missverständlich. Denn er ist nicht Ausfluss der mit der grundgesetzlichen Meinungsfreiheit einhergehenden Freiheit, sich aus allgemein zugänglichen Quellen zu informieren (Artikel 5 Abs. 1 Satz 1 GG), sondern eine Voraussetzung hierfür. Präziser, wenn auch im politischen Kontext weniger attraktiv, wäre deshalb die Bezeichnung Informationszugang oder - wie in Brandenburg – Akteneinsicht gewesen.

Im Anschluss an das Informationsfreiheitsgesetz des Bundes wurden in vielen Bundesländern ebenfalls Informationsfreiheitsgesetze erlassen. Bayern gehört bisher nicht dazu.

Kritik an diesem Gesetz stützt sich darauf, dass viele Ausnahmetatbestände enthalten sind, durch die das Recht auf Informationszugang eingeschränkt oder ganz verweigert werden kann.

Aufgrund seiner Zielrichtung gegen Bundesbehörden können die sich aus dem Informationsfreiheitsgesetz ergebenden Ansprüche weder gegen die Landeszentrale noch ihre Anbieter gerichtet werden.

²³ BGBl. I 2005, S 2722

2.2.9. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität

Am 11. August 2007 trat das 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (StrÄndG)²⁴ in Kraft. Hintergrund der Gesetzesänderung waren internationale Vorgaben zur Verbesserung der IT- Sicherheit.²⁵ Durch das Gesetz werden Straftatbestände ergänzt bzw. novelliert, die den Kernbereich des materiellen Computerstrafrechts darstellen. Es geht um die Vertraulichkeit, Integrität und Verfügbarkeit von Datensystemen.

So ist nunmehr bereits der unbefugte Zugang zu besonders gesicherten Daten unter Überwindung von Sicherheitsvorkehrungen in § 202a StGB unter Strafe gestellt. Es ist nicht notwendig, sich Daten zu verschaffen; es genügt, den Zugang zu verschaffen. Hacking ist somit strafbar.

Computersabotage (§ 303b StGB) war bisher nur bei Angriffen im gewerblichen Bereich strafbar. Nunmehr erstreckt sich der Tatbestand auch auf private Datenverarbeitungen. Zudem werden Störungen durch unbefugtes Eingeben und Übermitteln von Computerdaten unter Strafe gestellt. Damit sollen die Fälle abgedeckt werden, bei denen Server durch eine Vielzahl von Anfragen so belastet werden, dass die berechnete Kontaktaufnahme mit dem Server vereitelt oder zumindest erschwert wird.

Durch den neuen § 202b StGB wird auch unter Strafe gestellt, sich Daten aus einer nichtöffentlichen Datenübermittlung oder aus einer elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage unbefugt zu verschaffen.

Der neue § 202c StGB sanktioniert zudem das Herstellen, Überlassen, Verbreiten oder Verschaffen von „Hacker-Tools“, die bereits nach Art und Weise ihres Aufbaus darauf angelegt sind, illegalen Zwecken zu dienen. Umstritten ist hier, wie Tools zu behandeln sind, die neben rechtswidrigen auch zu rechtmäßigen Zwecken eingesetzt werden können.

Auch nach dieser Gesetzesänderung ist umstritten, ob das Phishing²⁶ von den Regelungen umfasst ist. Unter Phishing versteht man den Versuch, den Empfänger per E-mail irre zu führen und zur Herausgabe von Zugangsdaten und Passwörtern zu bewegen. Häufig wird dies mittlerweile

²⁴ BGBl. I 2007, S. 1786

²⁵ etwa Übereinkommen über Computerkriminalität des Europarats vom 23.11.2001; Rahmenbeschluss 2005/222/JI der EU

²⁶ vgl. dazu Graf, NSfZ, 2007, 129, Fn. 1

auch durch Trojaner versucht, die über E-Mails zum Empfänger gelangen und seinen Computer nach Zugangsdaten und Codes ausspähen, sie abspeichern und via Internet an die Täter übermitteln. Phishing kann aber auch über das Telefon erfolgen.

2.3 Bayerisches Landesrecht

2.3.1 Rundfunkstaatsvertrag (RStV)

Im Jahr 2005 war bereits über Entwürfe des 9. Rundfunkänderungsstaatsvertrags diskutiert und solche zur Anhörung an die voraussichtlich Betroffenen verschickt worden. Eine Ratifizierung unterblieb aber zunächst, weil die Europäische Kommission im Rahmen der Notifizierung verschiedene Bedenken im Hinblick auf Regelungen der E-Commerce-Richtlinie geäußert und Bund und Länder zu einer Klarstellung aufgefordert hatte. Diese Fragen wurden ausgeräumt, so dass der 9. Rundfunkänderungsstaatsvertrag²⁷ wie auch das ELGVG²⁸ einschließlich des Telemediengesetzes am 1. März 2007 in Kraft getreten ist²⁹.

Neben den oben geschilderten bundesrechtlichen wirtschaftsbezogenen Bestimmungen, die insbesondere im Telemediengesetz enthalten sind, sind mit dem 9. Rundfunkänderungsstaatsvertrag darüber hinausgehende inhaltespezifische Regelungen für Telemedien in einem neugefassten VI. Abschnitt des Rundfunkstaatsvertrags in Kraft getreten. Gleichzeitig trat mit dem 9. Rundfunkänderungsstaatsvertrag der Mediendienste-Staatsvertrag außer Kraft.

Seit dem 1. März 2007 richten sich die datenschutzrechtlichen Anforderungen auch hinsichtlich des Rundfunks nach den Vorschriften des Abschnitts Datenschutz des Telemediengesetzes (TMG) in seiner jeweilig geltenden Fassung³⁰. Wie oben unter 2.2.6 bereits angesprochen zeichnen sich die vom Bundesgesetzgeber weitgehend aus dem Bereich der Teledienste übernommenen Regeln nicht durch eine besondere Berücksichtigung rundfunkrechtlicher Gesichtspunkte aus, was möglicher Weise in dem Grundarrangement zwischen Bund und Ländern bereits angelegt ist, das dem für Rundfunk nicht zuständigen Bund die Hoheit über die auch im Rundfunk anzuwendenden Datenschutzregeln überlässt.

²⁷ BayGVBl 2007 S. 132.

²⁸ Vgl. oben unter 2.2.6

²⁹ Vgl. oben unter 2.2.6

³⁰ Vgl. § 47 Abs. 1 RStV n.F.

Umso mehr muss bei der Anwendung der Regeln darauf geachtet werden, dass die grundrechtlichen geschützten Positionen und Interessen insbesondere der Rundfunkfreiheit hinreichend beachtet werden.

Lediglich für diejenigen Daten, die ausschließlich eigenen journalistisch-redaktionellen Zwecken dienen, sind weiterhin Sonderregelungen im Rundfunkstaatsvertrag³¹ enthalten, so dass jedenfalls insoweit keine bedeutsame Änderung im Verhältnis zur bisher geltenden Rechtslage eingetreten ist und sich die oben genannten Fragen hier nur in geringerer Intensität stellen.

Durch die Aufhebung des MDStV finden sich nunmehr in §§ 54ff RStV die inhaltsbezogenen Regelungen für Telemedien. Gemäß § 59 Abs. 2 RStV ist für die Aufsicht eine nach dem Landesrecht bestimmte Stelle zuständig. Die Länder konnten sich somit weiterhin nicht für einen einheitlichen Weg entscheiden. Die bisher schon bestehenden Aufgabenzuweisungen wurden weitestgehend bestätigt; daher bestehen die unterschiedlichen Verhältnisse in den Ländern weiter, die insbesondere bei länderübergreifenden Zusammenhängen mit Rundfunkbezug zu überraschenden Ergebnissen führen, die durch den Betroffenen in der Regel nur schwer zu durchschauen sind.

Dies gilt insbesondere für die datenschutzrechtliche Aufsicht, die den nach den allgemeinen Datenschutzgesetzen zuständigen Kontrollbehörden übertragen ist³². Eine Neuerung ergibt sich allerdings dahingehend, dass auch für den Bereich der Telemedien die rundfunkrechtlichen Datenschutzbeauftragten des öffentlich-rechtlichen Rundfunks erstmals Erwähnung im Rundfunkstaatsvertrag finden, denen der Datenschutz im journalistisch-redaktionellen Bereich auch für die Telemedien übertragen wird.

Da auch die Landeszentrale öffentlich-rechtlicher Rundfunkveranstalter ist und dieser Erkenntnis folgend die Datenschutzaufsicht bei der Landeszentrale und ihren Anbietern derjenigen beim Bayerischen Rundfunk nachgebildet ist, wird diese Bestimmung auch für die Landeszentrale Bedeutung haben und Gültigkeit beanspruchen können. Eine klarstellende Anpassung der datenschutzrechtlichen Regeln des BayMG wäre insoweit jedoch zu begrüßen.

³¹ Vgl. § 47 Abs. 2 RStV n.F.

³² Vgl. § 59 Abs. 1 RStV n.F.

2.3.2 Bayerisches Mediengesetz (BayMG)

Das Bayerische Mediengesetz (BayMG) wurde im Berichtszeitraum der Jahre 2006 und 2007 zwar redaktionell und inhaltlich an die Vorgaben des RStV angepasst. Dies entfaltete aber keine datenschutzrechtlichen Wirkungen.

2.3.3 Gesetz zur Ausführung des Rundfunkstaatsvertrags und des Jugendmedienschutz-Staatsvertrags

Aufgrund der Aufhebung des MDStV musste auch das vorherige „Gesetz zur Ausführung des Mediendienste-Staatsvertrags und des Jugendmedienschutz-Staatsvertrags“ geändert werden. Diese Änderung geschah durch Gesetz mit Wirkung zum 01. März 2007.³³ Es handelte sich aber nur eine Fortschreibung von Zuständigkeiten. Die Zuständigkeit für die generelle Aufsicht über Telemedien einschließlich des Datenschutzes verblieb bei der Regierung von Mittelfranken.

³³ BayGVBl. 2007, S. 720

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 Rechtssprechung 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 bei diesem eine genaue Kenntnis der rechtlichen, wirtschaftlichen und programmlichen Verhältnisse besteht. Ferner ist eine Abgrenzung zwischen Erhebung, Verarbeitung und Nutzung personenbezogener Daten, die dem Medienprivileg unterfallen, und Verwaltungsangelegenheiten der Landeszentrale und der Anbieter entbehrlich, da die Aufsicht in einer Hand zusammengefasst ist.

Der Beauftragte für den Datenschutz bei der Landeszentrale überwacht nach Art. 20 Abs. 3 Satz 2 BayMG die Einhaltung der Vorschriften des BayMG sowie anderer Vorschriften über den Datenschutz bei der Landeszentrale und ihren Anbietern umfassend³⁴, und zwar auch soweit es sich um Verwaltungsangelegenheiten handelt, vgl. Art. 20 Abs. 3 Satz 3 BayMG. Mit dieser umfassenden Zuständigkeit für alle Aufgaben bei der Landeszentrale und den Anbietern trägt das BayMG den verfassungsrechtlichen Anforderungen an rundfunkrechtlichen Datenschutz Rechnung³⁵.

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

Der Beauftragten hat bei der Durchführung seiner Aufgaben Auskunfts-, Kontroll-, Zugriffs-, Einsichts- und Beanstandungsrechte.

³⁴ 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.

³⁵ Zu dieser Thematik hat der Norddeutsche Rundfunk ein sehr instruktives Gutachten bei Prof. Dr. Dieter Dörr erstellen lassen und 2002 als Band 13 der „Studien zum deutschen und europäischen Medienrecht“ veröffentlicht. Es trägt den Titel: „Rundfunk und Datenschutz – Die Stellung des Datenschutzbeauftragten des Norddeutschen Rundfunks“.

Der Beauftragte 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 Datenschutzregelungen 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 ihm keine Weisungen, insbesondere auch nicht vom Präsidenten oder dem Verwaltungsrat erteilt werden, die sich auf seine Aufgabenerfüllung beziehen. Die Stellung des Beauftragten für den Datenschutz bei der Landeszentrale entspricht damit der eines Richters.

Die Ausgestaltung der Datenschutzaufsicht nach dem BayMG dürfte somit auch zweifelsfrei den Anforderungen der EU-Datenschutzrichtlinie³⁶ entsprechen, die in Art. 28 Abs. 1 den Mitgliedstaaten auferlegt, datenschutzrechtliche Kontrollstellen zu schaffen, die die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahrnehmen. Die Erfüllung dieser Vorgabe ist für die Aufsicht über den nicht-staatlichen Bereich in der Bundesrepublik nicht unumstritten, denn die Europäische Kommission hat 5. Juli 2005 ein Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland eingeleitet³⁷, in dem die Kommission moniert, dass die Datenschutzaufsicht über die Privatwirtschaft, so wie sie derzeit organisiert sei, nicht in allen Fällen über die geforderte „völlige Unabhängigkeit“ verfüge. Die Gestaltung nach dem BayMG wurde dabei nicht angesprochen; die Landeszentrale ist von diesem Verfahren daher nicht betroffen. Das Verfahren vor dem Europäischen Gerichtshof dauert noch an; ein Termin für eine Entscheidung in der Sache ist derzeit noch nicht bekannt.

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

³⁶ Richtlinie 95/46/EG, ABl. EG v. 23.11.1995, Nr. L 281/31.

³⁷ Vgl. dazu oben 2.1.2.

4 Datenschutz in der Landeszentrale

4.1. Allgemeines

4.1.1. Datenschutzrechtliche Freigabe automatisierter Verfahren nach Art. 26 BayDSG

Die Landeszentrale ist gemäß 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 wurde ein automatisiertes Verfahren in diesem Sinne neu eingeführt; im Zusammenhang mit der Ersatzbeschaffung einer Telekommunikationsanlage wurde auch das für deren Betrieb eingesetzte System ausgetauscht, in welchem auch personenbezogene Daten für den Betrieb der TK-Anlage gespeichert und verarbeitet werden. Der Beauftragte für den Datenschutz war im Vorfeld der Einführung des Verfahrens eingebunden worden.

4.1.2. Verzeichnisse nach Art. 27 BayDSG

Die Landeszentrale führt gemäß 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 dem EDV-Abteilung vereinbart, dass dieses Anlageverzeichnis in gewisser Weise fortgeführt wird. Ein Verwaltungsmehraufwand entsteht hierdurch nicht, da die eingesetzte Hardware sowie die Peripherie-Geräte weiter inventarisiert und als Anlagevermögen aktiviert werden und daher im Anlageverzeichnis gemäß § 268 Abs. 2 HGB geführt werden müssen. Der Anlageverzeichnis unterstützt insoweit auch Planungen bei der Entwicklung von Konzepten auf dem Gebiet der Datensicherheit.

4.2. Verwaltungsgebäude der Landeszentrale

Das schon vor Beginn des Berichtszeitraumes 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 unterdessen 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 selbstständig und umgehend an den Beauftragten für den Datenschutz.

4.4. Umgang mit personenbezogenen Daten

Der Umgang mit personenbezogenen Daten erfolgt in der Landeszentrale prinzipiell auf Grundlage der zum Datenschutz erlassenen Dienstanweisung, die auch die in diesem Zusammenhang bedeutsamen Belange im Hinblick auf den Aspekt der Datensicherheit anspricht. Eine Überarbeitung war zuletzt im Zusammenhang mit der Novellierung des BayDSG in den Jahren 2000 und 2001 erforderlich gewesen. Weitere grundlegende Änderungen des geltenden Rechtes, die eine Änderung der seinerzeit überarbeiteten und durch die Geschäftsführung erlassene Dienstanweisung erforderlich gemacht hätten, waren nicht eingetreten, so dass die Dienstanweisung im aktuellen Berichtszeitraum keiner erneuten Änderung unterzogen werden musste.

Der Umgang mit personenbezogenen Daten im Einzelnen ist geprägt durch ein vergleichsweise hohes Maß an Sensibilisierung gegenüber datenschutzrechtlichen Fragestellungen und baut auf einem guten Kenntnisstand in Bezug auf

datenschützerische Herausforderungen auf. Dies belegen die laufenden Erfahrungen mit der Erfassung neuer Daten, Nutzungsänderungen oder Fragen der Weitergabe von Datenbeständen an Dritte, die in aller Regel mit dem Beauftragten für den Datenschutz bei der Landeszentrale abgestimmt und im Übrigen soweit ersichtlich von den Bereichen sachgemäß und unter Beachtung der Belange des Datenschutzes durchgeführt werden. Neue Konzepte und Planungen, die im Zusammenhang mit der Verarbeitung von personenbezogenen Daten stehen, werden in der Regel frühzeitig mit dem Beauftragten für den Datenschutz bei der Landeszentrale abgestimmt. Offene Fragen waren lediglich in einem Fall aufgetreten, die aber auch alsbald gelöst werden konnten. Insgesamt kann das Datenschutzniveau bei der Landeszentrale daher als hoch bezeichnet werden.

4.5. Auskunftersuchen, Anfragen, Beschwerden

Externen Auskunftersuchen im Hinblick auf Datenbestände der Landeszentrale waren im Berichtszeitraum nicht zu verzeichnen. Externe Anfragen wurden an den Beauftragten für den Datenschutz bei der Landeszentrale in einem deutlich steigenden Ausmaß gerichtet, waren zumeist allgemein gehaltene, konnten aber zumeist fermündlich beantwortet oder erledigt werden.

Insgesamt dokumentieren diese jedoch die stetig wachsende Aufmerksamkeit, die datenschutzrechtlichen Fragestellungen unterdessen entgegengebracht wird. Gewisse Komplikationen ergeben sich aus der Kombination der beiden nicht ganz alltäglichen Rechtsgebiete Datenschutz und Rundfunkrecht, die durch die Verbindung von technischen, wirtschaftlichen und rechtlichen Fragestellungen mit den gelegentlich ungewöhnliche Lösungsansätzen des Rundfunkrechtes (insbesondere in Zuständigkeitsfragen) für durchschnittliche Nutzer bzw. Anwender zu zum Teil nicht ohne Weiteres naheliegenden Antworten führt. In diesem Zusammenhang war der Beauftragte für den Datenschutz bei der Landeszentrale vom Arbeitskreis Medien des Düsseldorfer Kreis der Datenschutzaufsichtsbehörden zu einem Vortrag über die Besonderheiten des Rundfunkrechtes, der Rundfunkorganisation und der Rundfunknutzung zu deren Sitzung im Oktober 2006 in Berlin eingeladen worden, in der sich neben der geschilderten Thematik vor allem auch die besonderen Herausforderungen der unterschiedlichen von den Ländern gewählten Organisationssysteme für Datenschutz- und Rundfunkaufsicht zeigte.

Wegen datenschutzrechtlicher Fragestellungen im Hinblick auf die Tätigkeit der Landeszentrale selbst war beim Beauftragten für den Datenschutz bei der Landeszentrale im Berichtszeitraum lediglich eine Beschwerde gemäß Art. 20 Abs. 5

BayMG eingegangen, deren Vorbringen sich inhaltlich jedoch nicht als zutreffend erwies, so dass Schlussfolgerungen oder Konsequenzen nicht veranlasst waren.

4.6. Datensicherheit

Wie auch in den vorangegangenen Berichtszeiträumen hat sich die Landeszentrale auch in diesem fortlaufend um eine ständige Verbesserung der Datensicherheit bemüht. Ein Dauerthema auf diesem Gebiet sind die so genannten Computerviren und andere schädigende Programme, die wiederum ein erhöhtes Maß an Aufmerksamkeit erforderten.

Ziel dieser Attacken waren häufig tatsächliche und vermeintliche Sicherheitslücken der eingesetzten Softwareprodukte. Die bei der Landeszentrale eingesetzten Rechner sind für diesen Fall auf verschiedenen Ebenen mit entsprechenden Vorkehrungen versehen; zudem wurde durch den Einsatz der jeweils aktuellen Updates wie auch weiterer zusätzlicher Sicherheitsprogramme insbesondere für die Internetnutzung und den E-Mail-Verkehr eine nochmals verbesserte Sicherheitslage geschaffen, in der nennenswert erfolgreiche Angriffe auf die Server- und Netzwerkstrukturen im Berichtszeitraum ausgeschlossen werden konnten. Die bei der Landeszentrale eingesetzten Sicherungsmechanismen erwiesen sich durchwegs als wirkungsvoll. Im Berichtszeitraum war es, soweit ersichtlich, stets gelungen, eingehende schädigende Programme bereits im Vorfeld zu isolieren, so dass eine Schädigung der eingesetzten Programme bzw. der gespeicherten Daten oder gar eine unbefugte Nutzung dieser Daten nicht aufgetreten ist.

Gleichwohl gilt weiterhin der Grundsatz, dass man sich auch künftig fortlaufend um ein hohes Maß an Sicherheit bemühen und die erforderlichen Maßnahmen insbesondere beim Datenaustausch treffen muss. Die Landeszentrale hat dies in der Vergangenheit beherzigt, entsprechende Vorkehrungen getroffen und nimmt auch weiterhin laufende Anpassungen der Sicherungsmechanismen vor, um auf die sich laufend verändernden Bedrohungsszenarien ausreichend vorbereitet zu sein.

5. Datenschutz bei den Anbietern und Tochtergesellschaften der Landeszentrale

Im Zentrum meiner Tätigkeit gegenüber den Anbietern und Tochtergesellschaften der Landeszentrale stand einerseits wie in den Vorjahren die Beratung in Fragen des Datenschutzes und insbesondere hinsichtlich der sich aus den gesetzlichen Vorgaben ergebenden Anforderungen für die Gestaltung des betrieblichen Ablaufs.

Hinzu kam die laufende Beratung in einzelnen Fragen des Datenschutzes aus zumeist aktuellem Anlass. Die dabei bedeutsamen Fragen waren weiterhin vielfältig und reichten von den Voraussetzungen und erforderlichen Qualifikationen für eine Bestellung zum Datenschutzbeauftragten, der Zulässigkeit und den Vorzügen eines externer Datenschutzbeauftragten, und den sich aus einer Bestellung zum Datenschutzbeauftragten ergebenden arbeitsrechtlichen Folgen, über Fragen der internen E-Mail- und Internet-Nutzung bis zur Erforderlichkeit und zum Inhalt von Notfallhandbüchern. Diese Fragen konnten in der Regel telefonisch oder durch Versendung von Informationsmaterial geklärt werden.

Eine deutlich zunehmende Rolle spielte andererseits aber auch die Beratung der Anbieter vor Ort zumeist im Zusammenhang mit der Erörterung von Beschwerden, der sich in Einzelfällen auch die Überprüfung der Verhältnisse des einzelnen Anbieters anschloss. Dabei konnte festgestellt werden, dass die Anbieter über die datenschutzrechtlichen Erfordernissen in aller Regel gut informiert sind, diesen sehr aufgeschlossen gegenüber stehen und zumeist bereits eigenständig die notwendigen organisatorischen Vorkehrungen auch für ggf. erforderlich werdende verbesserte Sicherungsmaßnahmen getroffen oder zumindest vorbereitet haben.

Eine gewisse Rolle spielte der Umgang mit der reichhaltigen Menge der bei Call-In-Formaten gesammelten Daten. Fragen eröffnen sich einerseits im Hinblick auf den Zugang und die Weitergabe dieser Daten wie auch andererseits bezüglich der Auswertung und Verdichtung dieser Daten zu Nutzungs- oder Nutzerprofilen. In diese Richtung zielten auch zwei Beschwerden die in diesem Zusammenhang beim Beauftragten für den Datenschutz bei der Landeszentrale eingingen. Den Anliegen war im Folgenden Rechnung getragen worden. Die sich anschließenden Überprüfungen bei den betroffenen Anbietern verliefen in der oben geschilderten Art und Weise.

Einen Schwerpunkt bildeten die bei Pay-TV-Anbietern erhobenen Daten ihrer Nutzer und der Umgang mit diesen, was im Berichtszeitraum zu mehreren Beschwerden beim Beauftragten für den Datenschutz bei der Landeszentrale geführt hatte. Einen neuralgischen Punkt bildete einerseits der Umgang mit personenbezogenen Daten in Massenverfahren und insbesondere in Callcentern, die wegen der zumeist eingesetzten großen Anzahl von Mitarbeitern einen erheblichen Schulungsbedarf mit sich bringen. Grundlegende organisatorische Mängel konnten jedoch nicht festgestellt werden. Vielmehr

hatten die angesprochenen Anbieter bereits im Vorfeld Maßnahmen ergriffen, um den Schutz vor weiteren Datenschutzverstößen zu erhöhen bzw. diese prinzipiell auszuschließen.

Andererseits war im Rahmen des Vollzuges eines komplexen Dauerschuldverhältnisses ein Programmierfehler im Zusammenhang mit einem seinerzeit regelmäßig durchgeführten Datenabgleich unterlaufen, der zu einer Reihe von fehlerhaften Datenbeständen und sich daraus ergebenden unerwünschten Folgewirkungen für zahlreiche Kunden geführt hatte. Insbesondere daraus resultierte eine das Normalmaß der vorangegangenen Jahre deutlich übersteigende Anzahl von zu bearbeitenden Beschwerden. Da der Vorgang vor allem auch komplizierte technische Fragen aufwirft und zudem auch noch mehrere Unternehmen mit unterschiedlichen zuständigen Aufsichtsinstitutionen betrifft, war eine umfängliche Prüfung dieses Vorgangs notwendig geworden, die noch zu keinem abschließenden Ergebnis geführt hat. Dementsprechend war bisher auch keine abschließende Würdigung möglich.

Im Hinblick auf die übrigen Fragestellungen konnten abgesehen von in Massenverfahren wohl immer auftretenden Unachtsamkeiten und menschlichen Fehlleistungen keine erkennbaren organisatorischen Mängel festgestellt werden. Auf die aufgetretenen Einzelfallprobleme war auch ohne Zutun des Beauftragten für den Datenschutz bei der Landeszentrale jeweils angemessen reagiert worden, so dass eine Beanstandung im Berichtszeitraum in keinem Fall erforderlich erschien.

6. Weiterbildung

Die kontinuierliche Weiterbildung beruht 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. Einen eigenen Vortrag hielt ich vor dem Arbeitskreis-Medien des Düsseldorfer Kreises der Datenschutzaufsichtsbehörden zu rundfunkrechtlichen und tatsächlichen Fragestellungen im Zusammenhang mit dem Datenschutzrecht.

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 über besondere Kenntnisse von der Arbeit der Anbieter und ihren Umfeldbedingungen verfügt, andererseits aber auch über die verfassungsrechtlich geforderte Unabhängigkeit, die den Rundfunkbereich auszeichnet. Der Umstand, dass diese Konstruktion zumindest in 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.