



Der Bayerische Landesbeauftragte für den Datenschutz informiert zum Thema

Tätigkeitsbericht 2010

Pressemitteilung – Seite 1/8
München, 01.02.2011

Der Bayerische Landesbeauftragte für den Datenschutz, Dr. Thomas Petri, hat heute seinen 24. Tätigkeitsbericht 2010 vorgestellt.

Neben den Grundsatzthemen des Berichtes

- Reformen im Datenschutzrecht – Reformbedarf im Freistaat Bayern
- Vorratsspeicherung von Telekommunikationsverkehrsdaten
- Handlungspflichten aus dem neuen IT-Grundrecht
- Zentralisierung der staatlichen Datenverarbeitung
- Einführung des elektronischen Personalausweises
- Volkszählung 2011

enthält der Bericht zahlreiche Beiträge zur Gesetzgebung und Rechtsprechung, zu Bürgerbeschwerden und Überprüfungen von Amts wegen bei bayerischen öffentlichen Stellen.

Am 1. Dezember 2009 ist der Vertrag von Lissabon in Kraft getreten, der auch für den Datenschutz erhebliche Änderungen gebracht hat. Mit der neuen Ordnung ist auch die Charta der Grundrechte der Europäischen Union rechtsverbindlich geworden, die ein **Europäisches Grundrecht auf Datenschutz** gewährleistet. Aus Sicht des Bayerischen Landesbeauftragten für den Datenschutz ist dieses neue Europäische Grundrecht ein wesentlicher Fortschritt für den Datenschutz auch in Deutschland (1.2.1 - S. 13 - 14).



Pressemitteilung vom 01.02.2011 – Seite 2/8
Der Bayerische Landesbeauftragte für den Datenschutz informiert

Auf Bundesebene wurde das **Bundesdatenschutzgesetz** im Jahr 2009 gleich dreimal geändert. Soweit die Änderungen vergleichbare Sachverhalte betreffen, wäre eine Anpassung der Regelungen im Bayerischen Datenschutzgesetz zu empfehlen. Das gilt insbesondere für moderne Datenschutzgrundsätze und die Neuregelung zur Auftragsdatenverarbeitung (1.2.6 - S. 18 - 20). Wegen möglicher Auswirkungen auf bayerische Stellen ist auch das Gesetzgebungsverfahren für die **Neuregelung des Beschäftigtendatenschutzes** sorgfältig zu beobachten (1.2.7 - S. 20 - 23).

Im Freistaat Bayern ist das bewährte **Bayerische Datenschutzgesetz in die Jahre gekommen**. Es besteht ein erheblicher Änderungsbedarf, damit das Bayerische Datenschutzgesetz auch in Ansehung der technischen Entwicklung der letzten Jahre sachgerechte Lösungen auf die drängenden datenschutzrechtlichen Fragen der Gegenwart gibt. Dazu zählen beispielsweise Regelungen zum Umgang mit personenbezogenen Daten im Internet. Dringend ist auch eine angemessene Begrenzung von sogenannten **Verbunddateien**. Derartige Datenbanken werden von vielen Stellen gemeinsam genutzt und enthalten daher ein besonderes Gefährdungspotenzial für die erfassten Personen. Der Bayerische Landesbeauftragte für den Datenschutz appelliert an die Bayerische Staatsregierung, einen bereits vorhandenen Ressortentwurf möglichst zeitnah in den parlamentarischen Gesetzgebungsprozess zu überführen (1.2 - S. 13). Reformbedarf löst auch eine Entscheidung des Europäischen Gerichtshofs aus, nach der die bisherigen gesetzlichen Regelungen in Bayern nicht den europarechtlichen Anforderungen an eine völlig unabhängige Datenschutzaufsicht über die Privatwirtschaft genügen. Insoweit ist noch nicht abschließend geklärt, wie künftig die Datenschutzaufsicht im nicht-öffentlichen Bereich geregelt werden soll. Es wäre wünschenswert, wenn der Gesetzgeber sich bei seiner Neugestaltung der Datenschutzkontrolle von dem Leitbild eines effektiven institutionellen Datenschutzes führen ließe (1.2.5 - S. 16 - 18).

Das Bundesverfassungsgericht hat in seinem Urteil vom 2. März 2010 die gesetzlichen Vorschriften zur **Vorratsspeicherung von Telekommunikationsverkehrsdaten** durch die Anbieter von öffentlich zugänglichen Telekommunikations-, E-Mail- und Internetzugangsdiensten für nichtig erklärt. Sicherheitsbehörden tragen zwar immer wieder die Notwendigkeit einer Vorratsspeicherung von Telekommunikationsverkehrsdaten vor. Abgese-



hen von spektakulären Einzelfällen fehlt jedoch der konkrete Nachweis dafür, dass die Sicherheitslage in Deutschland ohne eine sechsmonatige Vorratsspeicherung sämtlicher Telekommunikationsverkehrsdaten nachhaltig verschlechtert wird. Die Möglichkeit von Sicherheitsbehörden, bei strafrechtlich relevanten Sachverhalten die Anbieter von Telekommunikations-Dienstleistungen zu einem „Einfrieren“ vorhandener Daten zu verpflichten, sollte als Alternative zur Vorratsspeicherung ernsthaft geprüft werden (1.2.4 - S. 16, 71 - 73).

Auch das neue Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (**IT-Grundrecht**) verpflichtet den Staat, auch im digitalen Zeitalter zu gewährleisten, dass vertraulich kommuniziert werden kann. Auf die Gesetzgeber kommt die Aufgabe zu, Regelungen zu schaffen, welche die Bürgerinnen und Bürger vor einer elektronischen Ausforschung schützen (2.1.1 - S. 25 - 27).

Gegenwärtig ist der Trend zu beobachten, dass die IT-Ressourcen des Freistaats in wenigen Standorten zusammengefasst werden. Durch diese **Zentralisierung der staatlichen Datenverarbeitung** erhofft man sich niedrigere Gesamtkosten. Auch wenn diese Zielsetzung nachvollziehbar ist, wirft die Grundsatzentscheidung unter dem Gesichtspunkt der Datensicherheit erhebliche Fragen auf. In datenschutzrechtlicher Hinsicht stößt eine ressortübergreifende Zentralisierung bestimmter IT-Aufgaben auch auf rechtliche Bedenken. So hat der Bayerische Landesbeauftragte für den Datenschutz sehr deutlich seine Skepsis gegen die zentrale Administration der Verzeichnisdienste (Active Directory) und die daraus folgende Zentralisierung von Exchange-Servern (elektronische Postfächer, Terminkalender, u.ä.) ausgesprochen (2.1.3 - S. 28 - 30). Hinsichtlich der Nutzung des sogenannten **Cloud Computing** werden die öffentlichen Stellen wegen der mit ihr verbundenen datenschutzrechtlichen Risiken zu äußerster Zurückhaltung aufgerufen (2.1.5 - S. 31 - 32).

Die **Einführung des elektronischen Personalausweises** wurde bereits im Rahmen des Feldtests begleitet. Mehrere Prüfungen haben ergeben, dass der Start des neuen Personalausweises auch aus datenschutzrechtlicher Sicht holprig ausgefallen ist. Bürgerinnen und Bürger wurden unzureichend informiert und die bei den Ausweisbehörden eingesetzten Lese-



und Schreibgeräte waren mangelbehaftet. Die abgegebenen Fingerabdruckdaten wurden zu lang gespeichert. Besonders misslich war dabei der Umstand, dass Antragsteller und die ausstellenden Behörden keine Möglichkeit hatten, die Korrektheit der abgegebenen Fingerabdruckdaten zu prüfen. Dabei verfolgt der neue Personalausweis durchaus auch Ziele, die aus datenschutzrechtlicher Sicht zu begrüßen sind. Neben der hohen Sicherheit des im Ausweis verwendeten RFID-Chips ist auch bei dem Zugriff auf Personalausweisdaten ein hoher Sicherheitsstandard geboten (2.3.1 - S. 53 - 56).

Die Vorbereitungen zur **Volkszählung 2011** laufen auf Hochtouren. Sowohl auf Bundes- als auch auf Landesebene haben die Landesbeauftragten für den Datenschutz sich intensiv in diese Vorbereitungsarbeiten eingebracht und konnten so erhebliche datenschutzrechtliche Verbesserungen für die Bürger erreichen. Die praktische Durchführung des Zensus wird der Bayerische Landesbeauftragte für den Datenschutz aus datenschutzrechtlicher Sicht auch weiterhin aufmerksam begleiten (12.1 - S. 194 - 196).

Neben diesen Themen sind folgende Ergebnisse der Kontrolltätigkeit hervorzuheben:

Ein Unternehmen der öffentlichen Daseinsvorsorge nahm **flächendeckend Drogentests bei der Einstellung neuer Mitarbeiter** vor. Datenschutzrechtlich zulässig ist nur, neu einzustellende Beschäftigte mit deren schriftlicher Einwilligung auf Alkohol- und Drogenabhängigkeit untersuchen zu lassen, sofern dies erforderlich ist, um die Eignung für die konkret vorgesehene Tätigkeit festzustellen. Ein flächendeckender Drogentest ist deshalb unzulässig (11.3 - S. 187 - 189).

DNA-Reihentests unter den Mitarbeitern wollte ein Finanzamt durchführen lassen, weil wiederholt obszöne und beleidigende Briefe an Beschäftigte vorgeblich von Kollegen abgesandt worden waren. Die Ermittlungen der zuvor eingeschalteten Polizei waren im Sande verlaufen. Die Finanzamtleitung musste darauf hingewiesen werden, dass derartige DNA-Untersuchungen allein dem strafrechtlichen Ermittlungsverfahren vorbehalten sind (11.6 - S. 191 - 192).



Pressemitteilung vom 01.02.2011 – Seite 5/8
Der Bayerische Landesbeauftragte für den Datenschutz informiert

Bereits vor einiger Zeit hat der Bayerische Landesbeauftragte für den Datenschutz darauf hingewiesen, dass die Erstellung von **personenbezieh- baren Benutzerstatistiken von Internetauftritten** datenschutzrechtlich im Regelfall unzulässig ist (Pressemitteilungen vom 06.09.2010 und vom 02.12.2010). Im Nachtrag zum Tätigkeitsbericht (2.1.6 - S. 32 - 34) kann jetzt mitgeteilt werden, dass nunmehr die ganz überwiegende Anzahl der öffentlichen Stellen die Hinweise des Bayerischen Landesbeauftragten für den Datenschutz umgesetzt hat.

Die **Datenspeicherung in polizeilichen Informationssystemen** bildete auch im Berichtszeitraum 2009/2010 einen Prüfungsschwerpunkt. Aus datenschutzrechtlicher Sicht ein Ärgernis bildet die Erfassung einer Frau, die trotz gerichtlichen Freispruchs wegen Verstößen gegen das Betäubungsmittelgesetz im **Kriminalaktennachweis** gespeichert wurde (3.5.3 - S. 76 - 77). In zwei weiteren Fällen wurde die Speicherung ihrer erkennungsdienstlichen Unterlagen unschuldigen Jugendlichen zum Verhängnis. In beiden Fällen haben die Betroffenen nichts zu ihrem Tatverdacht beigetragen (3.9 - S. 82 - 84). In allen beschriebenen Fällen nahm die Polizei auf Intervention des Bayerischen Landesbeauftragten für den Datenschutz im Nachgang die Löschung der Daten vor. Die Fälle unterstreichen erneut, dass strenge Regelungen zur polizeilichen Datenspeicherung im Interesse von unbescholtenen Bürgern notwendig sind.

Vor allem bei Sport-Großveranstaltungen wie der Leichtathletik-Weltmeisterschaft 2009, der FIFA U 20-Frauen-Weltmeisterschaft 2010 sowie aktuell der Ski-Weltmeisterschaft 2011 wurden **Zuverlässigkeitsüberprüfungen unter Einbindung von Sicherheitsbehörden** durchgeführt. So wurden die Daten von Betroffenen mit Dateien des Landeskriminalamtes und des Verfassungsschutzes abgeglichen. Als Rechtsgrundlage wurde erneut lediglich die Einwilligung der Betroffenen herangezogen. Bezüglich der Freiwilligkeit solcher Einwilligungen bestehen Zweifel, weil Betroffene oft unzumutbare Nachteile befürchten müssen, wenn sie ihre Einwilligung verweigern. Der Bayerische Landesbeauftragte für den Datenschutz weist darauf hin, dass die Verwaltung die wesentlichen Entscheidungen über die Voraussetzungen, Umstände und Folgen von Grundrechtseingriffen nicht an sich ziehen darf, sondern sie dem Gesetzgeber überlassen muss (3.11 - S. 85).



In zwei bekannt gewordenen Fällen wurden durch **Strafverfolgungsbehörden** Zeugen dazu veranlasst, **Hypnosesitzungen** durchführen zu lassen. In beiden Fällen wurde der Versuch unternommen, durch Hypnose festzustellen, ob sich ein Zeuge an ein Kfz-Kennzeichen erinnern könne. Selbst wenn die betroffenen Zeugen einem solchen Verfahren zustimmen, ist eine solche Vorgehensweise unzulässig, weil sie grundlegende Schutzvorschriften der Strafprozessordnung umgeht. Leider konnte insoweit kein Einvernehmen mit dem zuständigen Staatsministerium für Justiz und Verbraucherschutz erzielt werden (5.3.1 - S. 94 - 95).

Mehrere Eingaben betrafen **Kontenabfragen durch Staatsanwaltschaften**. In einem Fall wurde eine Kontenabfrage bereits zeitgleich mit der Beschuldigtenvernehmung angeordnet. In einem anderen Fall hatte die Staatsanwaltschaft Kontounterlagen eines nicht beschuldigten Rechtsanwalts angefordert, der diesem Verfahren nicht zugestimmt hatte. Diese Fälle geben Anlass für künftige Prüfungen in diesem Bereich (5.3.4 - S. 97 - 98).

In einer **Justizvollzugsanstalt** wohnten weibliche Vollzugsbeamte der ärztlichen Sprechstunde des Anstaltsarztes für weibliche Gefangene bei. Die Anwesenheit sei erforderlich, um den Anstaltsarzt vor ungerechtfertigten Anschuldigungen zu schützen. Der vom Bayerischen Landesbeauftragten für den Datenschutz vertretene Auffassung, dass eine solche Vorgehensweise die **ärztliche Schweigepflicht** berührt, schloss sich das Staatsministerium für Justiz und Verbraucherschutz an (5.4.2 - S. 99).

Die **Videoüberwachung in und an öffentlichen Gebäuden und Plätzen** stellte auch in diesem Berichtszeitraum einen erheblichen Teil der Kontrolltätigkeit dar. Bei Prüfungen ergaben sich häufig erhebliche Unsicherheiten im Umgang mit der neuen gesetzlichen Vorschrift zur Videoüberwachung im Bayerischen Datenschutzgesetz. Positiv zu erwähnen ist das Engagement der behördlichen Datenschutzbeauftragten einiger bayerischer Städte, die im Zusammenwirken mit dem Bayerischen Landesbeauftragten für den Datenschutz und einem Vertreter des Staatsministeriums des Innern Hilfestellungen erarbeitet haben. Diese Hilfestellungen sind auf der Webseite des Bayerischen Landesbeauftragten für den Datenschutz aufrufbar (6.1 bis 6.3 - S. 101 - 105).



Pressemitteilung vom 01.02.2011 – Seite 7/8

Der Bayerische Landesbeauftragte für den Datenschutz informiert

Die **Auskunftserteilung über Behördeninformanten** war im Berichtszeitraum Gegenstand mehrerer Beanstandungen gegenüber Kommunen. In einem Fall beschwerte sich ein 12-jähriger Junge bei einer Verwaltungsgemeinschaft, nachdem er von mehreren nicht angeleiteten Hunden einer Hundehalterin bedrängt worden war. Die Verwaltungsgemeinschaft wies daraufhin die Hundehalterin in allgemeiner Form auf die Anleinplicht hin. Auf deren Frage nach dem Anzeigeresteller gab die Verwaltungsgemeinschaft Name und Anschrift des Kindes bekannt. Die Hundehalterin wiederum suchte das Kind in Abwesenheit der Eltern auf und griff es in der Folge verbal an. Die Vorgehensweise der Verwaltungsgemeinschaft wurde als erheblicher datenschutzrechtlicher Verstoß beanstandet (6.10 - S. 112 - 114).

Der Medizinische Dienst der Krankenversicherung in Bayern betreibt im Auftrag der gesetzlichen Pflegekassen in Bayern den „**Pflegeservice Bayern**“, eine kostenlose Rufnummer für Pflegebedürftige. Bei dieser Servicenummer wurde erst am Ende des Telefonats und eher beiläufig mitgeteilt, das Gespräch werde zur Sicherheit der Anrufer aufgezeichnet. Eine Löschung erfolgte nur bei ausdrücklichem Widerspruch der betroffenen Anrufer. Diese datenschutzrechtlich unzulässige **Aufzeichnung von Telefongesprächen** wurde aufgrund der Intervention des Bayerischen Landesbeauftragten für den Datenschutz beendet (8.8 - S. 138 - 139).

In einem öffentlich zugänglichen **Internetportal** tauschten sich ARGE-Mitarbeiter über **Kindernamen von Sozialleistungsempfängern** aus. Diese Daten ließen zumindest in Einzelfällen Rückschlüsse auf die Identität konkreter Leistungsempfänger zu. Eine in Bayern betroffene ARGE entschuldigte sich bei den betroffenen Leistungsempfängern für diesen Verstoß gegen das Sozialgeheimnis (8.19 - S. 147).

Auch in diesem Berichtszeitraum musste mehrfach die datenschutzrechtlich verbotene **Weitergabe von Schülerdaten zu Werbezwecken** durch Schulen kritisiert werden. Das Staatsministerium für Unterricht und Kultus entsprach der Bitte des Bayerischen Landesbeauftragten für den Datenschutz und wies erneut mit Rundschreiben an alle bayerischen Öffentlichen Schulen auf das Verbot hin (10.4 - S. 167 - 169).



Pressemitteilung vom 01.02.2011 – Seite 8/8
Der Bayerische Landesbeauftragte für den Datenschutz informiert

Elektronische Fallakten werden gegenwärtig datenschutzrechtlich heftig diskutiert, weil sie auch klinikübergreifende Zugriffe auf Patientendaten ermöglichen. Soweit solche Datenzugriffe nur zu notwendigen Heilbehandlungen erfolgen könnten, wäre dies nicht zu beanstanden. Problematisch ist vor allem das erhebliche Risiko unzulässiger Zugriffe. Vor diesem Hintergrund führt das **Städtische Klinikum München** ein Modellprojekt durch, bei dem man den Bayerischen Landesbeauftragten für den Datenschutz von Beginn an eng eingebunden hat, um die datenschutzrechtlichen Anforderungen zu erfüllen (2.2.10 - S. 47 - 48).

Der Tätigkeitsbericht 2010 ist wie die vorangegangenen Tätigkeitsberichte des Bayerischen Landesbeauftragten für den Datenschutz im Internet unter www.datenschutz-bayern.de abrufbar.

Dr. Thomas Petri

Abdruck honorarfrei unter Quellenangabe, Belegexemplar erbeten