



# Der Bayerische Landesbeauftragte für den Datenschutz

---

## 26. Tätigkeitsbericht 2013/2014

---

Pressemitteilung – Seite 1/8  
München, 20.01.2015

Der Bayerische Landesbeauftragte für den Datenschutz, Dr. Thomas Petri, hat heute seinen 26. Tätigkeitsbericht für die Jahre 2013/2014 vorgestellt:

Neben Grundsatzthemen wie

- Neuordnung des Europäischen Datenschutzrechtsrahmens
- Vorratsdatenspeicherung
- Videoüberwachung in Bayern

enthält der Bericht zahlreiche Beiträge zur Gesetzgebung, zu Bürgerbeschwerden und zu Prüfungen bei bayerischen öffentlichen Stellen.

Vor über zwei Jahren veröffentlichte die Europäische Kommission **Vorschläge zur Neuordnung des Europäischen Datenschutzrechtsrahmens**. Die bisher für die EU-Mitgliedstaaten geltenden allgemeinen Datenschutzregeln sollen durch eine Datenschutz-Grundverordnung und durch eine Richtlinie für den Datenschutz im Bereich der Strafjustiz ersetzt werden. Mittlerweile hat das Europäische Parlament im Rahmen des Gesetzgebungsverfahrens eine eigene Verhandlungsposition entwickelt; auch der Rat strebt eine Verabschiedung der geplanten Neuregelung bis Ende 2015 an. Eine Reform des Europäischen Datenschutzrechtsrahmens ist nach wie vor dringend notwendig. Sie sollte allerdings den Mitgliedstaaten auch Gestaltungsspielräume für die Fortentwicklung des Datenschutzes eröffnen (Nr. 1.2.1, S. 18 - 20).

Angesichts der furchtbaren Ereignisse von Paris werden Stimmen laut, die eine Einführung der **Vorratspeicherung von Telekommunikations-Verkehrsdaten** in Deutschland fordern. Der Bericht verweist insoweit auf ein Urteil des Europäischen Gerichtshofs vom 8. April 2014, wonach die

---

Ihr Persönlichkeitsrecht - unser Auftrag

---



Pressemitteilung vom 20.01.2015 – Seite 2/8  
Der Bayerische Landesbeauftragte für den Datenschutz informiert

---

Einführung einer anlassfreien flächendeckenden Verkehrsdatenspeicherung unverhältnismäßig in die Grundrechte auf Privatheit und auf Datenschutz eingreifen würde (Nr. 1.2.2, S. 20 - 22, Nr. 3.1.3, S. 72).

Bereits in den vergangenen Jahren führte die **Videoüberwachung in Bayern** zu zahlreichen Beschwerden. Sie bildet daher seit jeher einen Schwerpunkt meiner Kontrolltätigkeit. Im Berichtszeitraum führte die Beantwortung einer parlamentarischen Anfrage zu einer Auflistung der Kamerateandorte bei bayerischen öffentlichen Stellen. Diese Liste habe ich systematisch auf Auffälligkeiten untersucht und bin ihnen im Wege von Prüfungen nachgegangen (Nr. 1.4.2, S. 31). Darüber hinaus habe ich einen mit dem Innenministerium abgestimmten Leitfaden entwickelt, der kurz und prägnant die insbesondere bei der kommunalen Videoüberwachung zu beachtenden Gesichtspunkte erläutert (Nr. 6.2, S. 120 - 123).

Über die Grundsatzthemen hinaus sind folgende Ergebnisse meiner Kontroll- und Beratungstätigkeit hervorzuheben:

Die **technische Sicherheit und die Wahrung der Vertraulichkeit bei der Datenübertragung** waren im Berichtszeitraum – nicht zuletzt vor dem Hintergrund der sogenannten NSA-Affäre – häufig medienbeherrschende Themen. Meine seit 1982 diesbezüglich regelmäßig gestellten Forderungen habe ich zusammengestellt und erneut erhoben (Nr. 2.1.1, S. 34 - 38). Die Notwendigkeit für geeignete **Verschlüsselungs- und Schutzmechanismen** sollte nun mittlerweile jedermann bewusst sein – es ist höchste Zeit, diese Mechanismen konsequent einzusetzen. In diese Richtung gehen auch die Bemühungen der bayerischen Verwaltung nach **sicherer E-Mail**, beispielsweise beim De-Mail-Pilotierungstest (Nr. 2.2.5, S. 51 - 53) und bei der Plattform für sichere Kommunikation in Bayern – BayMail (Nr. 2.2.6, S. 53 - 54). Während das De-Mail-Projekt noch nicht zu einem erfolgreichen Abschluss gebracht und eingeführt werden konnte, hat das Innenministerium für das Projekt BayMail zumindest eine bis 31.07.2018 zeitlich begrenzte Freigabe erteilt. Aber auch alle ergriffenen Sicherheits- und Schutzmechanismen müssen ständig aktuell gehalten und überprüft werden, wie unter anderem der zur Sicherung von Internetauftritten häufig verwendete Verschlüsselungsalgorithmus RC4 zeigt (Nr. 2.2.4, S. 48 - 51).



Wie in den vergangenen Jahren behandelt auch dieser Bericht ausführlich **Datenspeicherungen im polizeilichen Informationssystem (INPOL) bzw. im Kriminalaktennachweis (KAN)**. Sie sind grundsätzlich nur zulässig, wenn ein sogenannter **polizeilicher Restverdacht** bezüglich einer strafbaren Handlung weiterhin vorliegt. Bei den diesbezüglichen Prüfungen konzentrierte ich mich auf Ermittlungsverfahren, die von der Staatsanwaltschaft eingestellt wurden, da sich gegen den vormals Beschuldigten nach den Ermittlungen kein begründeter Tatverdacht mehr ergab. Dabei stellte ich fest, dass in vielen Fällen die Speicherung in der Vorgangsverwaltung der Polizei nicht dem Verfahrensausgang entsprechend angepasst wurde. In seltenen Fällen wurden ehemalige Beschuldigte sogar trotz der Feststellung des restlos entfallenen Tatverdachts weiterhin im KAN als Beschuldigte geführt. Meiner Aufforderung, die betroffenen Speicherungen zu ändern bzw. zu löschen, kamen die geprüften Polizeipräsidien nach (Nr. 3.5.3, S. 81 - 82). Zudem hat sich gezeigt, welche erhebliche Bedeutung die Mitteilung der Staatsanwaltschaft an die Polizei über den Ausgang des Verfahrens besitzt. Ich habe deshalb gegenüber den in diesem Zusammenhang ebenfalls geprüften Staatsanwaltschaften die Wichtigkeit korrekter Ausgangsmitteilungen hervorgehoben und sie auf die von mir in Einzelfällen festgestellten Versäumnisse hingewiesen (Nr. 5.3.5, S. 109 - 110).

Unzulässige Speicherungen können **gravierende Auswirkungen** für den Betroffenen haben: So wollte eine Fahrerlaubnisbehörde die Eignung einer Bürgerin zum Führen von Kraftfahrzeugen überprüfen, da gegen sie polizeiliche Ermittlungen aufgrund des Verdachts eines Betäubungsmitteldeliktes geführt wurden. Die Bürgerin war als Absenderin auf einem Brief genannt, der Drogen enthielt. Die Ermittlungen ergaben, dass ihr Name vom tatsächlichen – unbekanntem – Täter missbräuchlich verwendet wurde. Trotz der bereits von Anfang an schwachen Verdachtslage teilte die Polizei den Vorwurf gegen die unbeteiligte Bürgerin der zuständigen Fahrerlaubnisbehörde mit und speicherte sie auch nach der Einstellung des Verfahrens weiter als Beschuldigte. Die Polizei bedauerte den Vorfall und kam meiner Forderung nach, die Speicherung im Kriminalaktennachweis zu löschen (Nr. 3.5.6.3, S. 86 - 87).



Einen weiteren Prüfungsschwerpunkt setzte ich im Bereich der **erkenntnisdienstlichen Behandlungen**. Erkennungsdienstliche Behandlungen kommen typischerweise bei gewerbs- oder gewohnheitsmäßig handelnden Tätern in Betracht. Leider musste ich bei der Prüfung eines Polizeipräsidiums feststellen, dass dieser Grundsatz nicht ausreichend beachtet und zu viel sowie zu schnell erkenntnisdienstlich behandelt wurde. Beispielsweise war die erkenntnisdienstliche Behandlung eines Bürgers wegen zweier Ladendiebstähle geringwertiger Sachen nicht verhältnismäßig. Einmal entwendete er eine Packung Brotzeiteier und dreieinhalb Jahre später eine DVD im Wert von 8,99 Euro. Ich betone jedoch, dass diese Prüfung auch ein Beispiel für die erfreuliche Zusammenarbeit mit der Polizei in den vergangenen Jahren darstellt: Das geprüfte Polizeipräsidium folgte in allen Fällen meiner Aufforderung zur Löschung. Darüber hinaus hat es mir zugesichert, das Thema intern aufzubereiten und eine Verbesserung anzustreben (Nr. 3.5.4, S. 82 - 84).

Auch im Bereich des **Strafvollzugs** konnte ich datenschutzrechtliche Verbesserungen erreichen. So wurde beispielsweise in allen bayerischen Justizvollzugsanstalten für Gefangene die Möglichkeit geschaffen, genehmigte Telefonate mit ihren Verteidigern entsprechend der Gesetzeslage ohne inhaltliche Überwachung zu führen. Des Weiteren konnte ich die datenschutzrechtlichen Standards erhöhen, sofern in sogenannten Mutter-Kind-Abteilungen Daten über die Kinder der Gefangenen erhoben werden (Nr. 5.4, S. 110 - 112).

Ein **Kurort** hat gegen die gesetzliche Zweckbindung der in den Beherbergungsstätten erhobenen **Melddaten** verstoßen. Der Leiter der Tourist-Information hatte im Rahmen regelmäßig stattfindender sogenannter Hotel-Stammtische Listen mit den Ankunfts- und Übernachtungszahlen der größeren ortsansässigen Betriebe, getrennt nach den einzelnen Betrieben, an die bei dem Stammtisch anwesenden Hoteliers verteilt. Damit wollte er über die Tourismusentwicklung in der Gemeinde informieren. Diesen Hoteliers wurden damit wirtschaftliche Verhältnisse ihrer Konkurrenten bekannt. Zur Information über die Tourismusentwicklung in der Gemeinde wäre die Bekanntgabe der Ankunfts- und Übernachtungszahlen im Übrigen auch gar nicht erforderlich gewesen. Diesem Zweck dienen regelmäßig gerade die Fremdenverkehrsstatistiken (Nr. 6.7, S.129 - 130).



Eine **Gemeinde** hat bei der Weitergabe von **Melderegisterdaten zu Wahlwerbezwecken** gleich mehrfach gegen den Datenschutz verstoßen. So wurden zwar die Widersprüche eines Ehepaars, das sich an mich gewandt hatte, gegen eine derartige Datenübermittlung beachtet. Jedoch wurden die Meldedaten ihres zweijährigen Kindes an eine politische Partei weitergegeben. Unzulässig war auch die Weitergabe einer Liste aller Haushalte sowie der Geburtsdaten der betroffenen Bürger. Zu guter Letzt wurde in zehn Fällen auch noch Auskunft über nicht wahlberechtigte Personen erteilt (Nr. 6.15, S. 138 - 139).

Einen Schwerpunkt der **Kontrollen im Gesundheitswesen** bildete die breit angelegte Untersuchung von **Gesundheitsämtern**. Ein besonderes Interesse habe ich dabei auf die Frage gelegt, ob und in welcher Weise die gesetzlichen Geheimhaltungspflichten und Verwertungsverbote eingehalten werden, beispielsweise bei der gesundheitlichen Beratung für Menschen, die an einer Sucht oder an einer psychischen Krankheit leiden. Geprüft habe ich ferner, ob – wie es der Datenschutz fordert – die Aufgabenbereiche Medizinisches Gutachterwesen, Infektionsschutz und Hygiene sowie Gesundheitsförderung getrennt waren. Weitere Prüfgegenstände waren die Aktenverwaltung, die formularmäßige Verwendung von Einwilligungserklärungen in Untersuchungen und Erklärungen über die Entbindung von der ärztlichen Schweigepflicht sowie das Verfahren der verpflichtend vorgesehenen Impfberatungen in Schulen. Es ist mir gelungen, Verbesserungen in den angeführten Bereichen zu erzielen. Gleichwohl wird die weitere Optimierung der datenschutzrechtlichen Standards bei den Gesundheitsämtern auch weiterhin zu meinen Schwerpunkten gehören (Nr. 7.1.1 und 7.1.2, S. 140 - 145).

Im Gesundheitswesen, insbesondere in Kliniken und Gesundheitsämtern, lag auch eine Priorität der **technisch-organisatorischen Prüfungen**. Dabei ging es bei den Kliniken hauptsächlich um die praktische Umsetzung der im Jahr 2011 erstmalig veröffentlichten Orientierungshilfe **Krankenhausinformationssysteme** (Nr. 2.2.3, S. 47 - 48). Hier konnten erfreulicherweise einige Verbesserungen festgestellt werden, die sowohl auf Bemühungen der herstellenden Industrie als auch auf die die Software einsetzenden Häuser zurückzuführen sind. Noch nicht zufriedenstellend gelöst sind die Umsetzung des Widerspruchsrechts der Patienten zur Hinzu-



ziehung von Vorbehandlungsdaten und technische Funktionalitäten zur physikalischen Löschung von gespeicherten Daten. Bei den **Gesundheitsämtern** waren der Umgang mit den dortigen Datenverarbeitungssystemen und die Anbindung an die Datenverarbeitungssysteme des jeweiligen Landratsamtes bzw. der jeweiligen Kommune von besonderem Interesse. Auch hier gibt es noch Verbesserungspotential – meine seit Jahren bestehenden Forderungen habe ich aktualisiert und präzisiert (Nr. 2.2.2, S. 46 - 47). Im Gesundheitswesen ist eine gewisse Tendenz zur verstärkten Einbindung externer Dienstleister erkennbar. Dies zeigte sich im Berichtszeitraum z.B. in den Bereichen der Teleradiologie (Nr. 2.3.4, S. 60 - 61), des Backups von Radiologiedaten (Nr. 2.3.6, S. 61 - 62) und im Rettungswesen (Nr. 2.3.7, S. 62 - 63).

Im Sozialwesen lag der Fokus auf der **Prüfung von Krankenkassen und Medizinischem Dienst** der Krankenversicherung (MDK). In der Vergangenheit hat sich gezeigt, dass Krankenkassen insbesondere bei der Gewährung von Krankengeld nicht immer die ihnen im Sozialgesetzbuch vorgegebenen Grenzen bei der Erhebung, Verarbeitung und Nutzung der Versichertendaten eingehalten haben. Sie haben dabei z.B. besonders sensible Behandlungsunterlagen über ihre Versicherten angefordert, die grundsätzlich nur dem MDK vorbehalten sind. Nach vielen Gesprächen konnte ich Änderungen erreichen, die zu einem höheren Datenschutzniveau geführt haben (Nr. 8.1, S. 161 f., insbesondere Nr. 8.1.4, S. 164 - 165).

In Ablösung der herkömmlichen Papierlohnsteuerkarte werden seit 2013 beim Bundeszentralamt für Steuern die **Elektronischen Lohnsteuerabzugsmerkmale (ELStAM)** aller nichtselbstständig Beschäftigten für den automatisierten Abruf durch den Arbeitgeber bereitgestellt. Aus Datenschutzsicht möchte ich insbesondere darauf aufmerksam machen, dass jeder betroffene Bürger über sein Finanzamt die Bereitstellung der ELStAM allgemein sperren, nur für bestimmte Arbeitgeber freigeben (Positivliste) oder nur für bestimmte Arbeitgeber sperren (Negativliste) lassen kann. Dies kann dazu beitragen, unberechtigte (Neugier-)Abfragen zu verhindern (Nr. 9.1, S. 186 - 188).



Pressemitteilung vom 20.01.2015 – Seite 7/8  
Der Bayerische Landesbeauftragte für den Datenschutz informiert

---

Einen Schwerpunkt meiner Kontroll- und Beratungstätigkeit bildete im Berichtszeitraum erneut der **Datenschutz an Schulen**.

In den letzten Jahren hat an den bayerischen Schulen die Nutzung von **elektronischen Lernplattformen** stark zugenommen. Aufgrund der personalisierten Anmeldung einerseits und der Protokollierung aller Nutzungsbewegungen andererseits können hier allerdings detaillierte Verhaltensprofile der einzelnen Nutzer – Schülerinnen und Schüler wie Lehrkräfte – leicht erstellt werden. Mit dem Kultusministerium habe ich daher Nutzungsregelungen vereinbart, die den Datenschutzrechten der Betroffenen so weit wie möglich Rechnung tragen. Zudem darf ein Einsatz passwortgeschützter Lernplattformen nur unter sehr engen Maßgaben – dezentral von der jeweiligen Schule vor Ort – zum verpflichtenden Bestandteil des Unterrichts erklärt werden (Nr. 10.1.2, S. 192 - 194, und Nr. 10.3, S. 198 - 200).

Unklarheiten bestehen in der Praxis immer wieder darüber, welche Angaben die Schulen im Falle der **Erkrankung einer Schülerin oder eines Schülers** verlangen dürfen. So ist nicht allgemein bekannt, dass die Schulen – außer bei meldepflichtigen Erkrankungen – die Angabe der ärztlichen Diagnose oder der Krankheitsbezeichnung nicht fordern dürfen; vielmehr muss hier nur der Umstand der Erkrankung mitgeteilt werden (Nr. 10.5, S. 204 - 206).

Ein staatliches Museum musste ich darauf aufmerksam machen, dass die **Ausgabe von Audioguides** nicht von der **Hinterlegung des Personalausweises** oder eines anderen amtlichen Lichtbilddokumentes „als Pfand“ abhängig gemacht werden darf. Eine solche Forderung verstößt nicht nur gegen die Vorschriften des Personalausweisgesetzes, sondern ist in Anbetracht der Sensibilität der Personalausweisdaten auch datenschutzrechtlich äußerst problematisch (Nr. 10.11, S. 220 - 221).

Die **Nutzung Sozialer Medien durch bayerische Behörden** hat mich erneut intensiv beschäftigt (Nr. 12.4, S. 239 f.). Dies betrifft insbesondere die Einrichtung von Fanpages auf Facebook zum Zweck der Öffentlichkeitsarbeit, zumal hier weiterhin strittige Rechtsfragen bestehen (Nr. 12.4.1, S. 240 - 243). In einer anderen Fallgestaltung wollte eine



Pressemitteilung vom 20.01.2015 – Seite 8/8  
Der Bayerische Landesbeauftragte für den Datenschutz informiert

---

Behörde mittels eines eigenen Facebook-Accounts Bürger in geschlossenen Gruppen personenbezogen beraten. Da ich die Behörde auf die datenschutzrechtliche Unzulässigkeit des Projekts hingewiesen habe, hat sie hiervon Abstand genommen (Nr. 12.4.2, S. 243 - 244). Außerdem habe ich 5592 Webseiten bayerischer Behörden geprüft und erreicht, dass Social Plugins nicht mehr – unzulässig – direkt in Webseiten eingebunden werden. Bei einer der 66 zunächst auffälligen Stellen gelang dies erst, nachdem ich diese Stelle beanstandet hatte (Nr. 12.4.3, S. 244 - 245).

Ich empfehle bayerischen Behörden weiterhin, bei der Inanspruchnahme von **Cloud-Diensten** äußerste Zurückhaltung walten zu lassen. Bei Beratungen hat sich auch gezeigt, dass vorgelegte Vertragsbedingungen von Cloud-Anbietern nicht die Anforderungen erfüllt haben, die für bayerische Behörden maßgeblich sind (Nr. 13.1, S. 246 - 247).

Dr. Thomas Petri