



Baden-Württemberg

DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ

PRESSEMITTEILUNG

21. Januar 2014

Zwischen Big Brother und Big Data

Landesbeauftragter für den Datenschutz legt Tätigkeitsbericht vor.

Der Landesbeauftragte für den Datenschutz, Jörg Klingbeil, hat am 27. Januar 2014 seinen Tätigkeitsbericht vorgestellt, der die Jahre **2012** und **2013** umfasst. Der **Bericht im neuen Layout** ist - nach der Zusammenlegung der beiden Datenschutzaufsichtsbehörden in Baden-Württemberg zum 1. April 2011 - der zweite seiner Dienststelle, in dem auch der Datenschutz im nicht-öffentlichen Bereich behandelt wird.

Als **aktuelle Herausforderungen** für den Datenschutz bezeichnete Jörg Klingbeil die **Spähaffäre** angloamerikanischer Geheimdienste (vgl. Kapitel 1.1, S. 9 ff.) und die zunehmende massenhafte Datenspeicherung und -auswertung für unterschiedliche Zwecke („**Big Data**“, vgl. Kapitel 1.2, S. 15 ff.): „Das Jahr 2013 wird als das Jahr in die Geschichte eingehen, in dem das Internet seine Unschuld verloren hat. Die Ohnmacht Deutschlands auf politischer, rechtlicher und technischer Ebene ist durch die NSA-Affäre überdeutlich geworden. Die vom Bundesverfassungsgericht aufgerichteten Schranken (z.B. Grundrecht auf informationelle Selbstbestimmung und Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme) sind von den ausländischen Geheimdiensten ignoriert worden; man hat den Eindruck, dass das, was technisch geht, auch gemacht wird. Jetzt muss entschlossen gehandelt werden, um die Souveränität zurückzugewinnen. Dazu gehören eine rasche **europäische Datenschutzreform** und die **Aussetzung des Safe-Harbor-Abkommens**, das bestenfalls nur noch symbolische Bedeutung hat. Außerdem sind im **Transatlantischen Freihandelsabkommen (TTIP)** gleiche Datenschutzstandards für Amerikaner wie Europäer auszuhandeln. Parallel dazu sind **völkerrechtliche Abkommen zur Eindämmung von Geheimdienstaktivitäten** erforderlich, weil das

europäische Recht außereuropäische Geheimdienste nicht binden kann. Die kommende Datenschutz-Grundverordnung der EU wird mit ihrem Marktortprinzip zudem hoffentlich dafür sorgen, dass der Datenabfluss bei amerikanischen Anbietern transparenter wird.“

Der nationale Datenschutz sei in der Spähaffäre weitgehend hilflos, räumte der Landesbeauftragte ein: „Es ist schon frustrierend, wenn wir uns permanent um alltägliche Datenschutzprobleme kümmern - um die unerwünschte Werbe-E-Mail ebenso wie um den Nachbarstreit wegen einer Videokamera, um im Polizeicomputer gespeicherte „Jugendsünden“ ebenso wie um überquellende Behördenbriefkästen - und wenn das Bundesverfassungsgericht das Verbot einer Totalüberwachung zur verfassungsrechtlichen Identität unseres Landes rechnet, und auf der anderen Seite greifen ausländische Nachrichtendienste ungeniert auf den gesamten weltweiten Kommunikations- und Internetverkehr zu. Die Privatsphäre wird auf diese Weise ad absurdum geführt.“ Immerhin habe aber die NSA-Affäre wie ein Weckruf gewirkt und - wie Umfragen zeigten - das Bewusstsein für die Datensicherheit bei Privatleuten und in der Wirtschaft deutlich wachsen lassen. „Das Vertrauen in Angebote mit amerikanischer Beteiligung, z.B. bei Cloud Computing, hat massiv gelitten“, ergänzte Jörg Klingbeil, „gerade bei den mittelständischen Unternehmen in Baden-Württemberg ist eine erhebliche Verunsicherung zu spüren. Dieser Vertrauensverlust ist jetzt eine Chance für **Datenschutz made in Europe**“. Ob es sinnvolle nationale Lösungen für das Internet geben könne, sei dagegen eher zweifelhaft: „Wir können die Entwicklung nicht zurückdrehen, aber vielleicht doch mehr Kontrolle zurückerlangen, z. B. durch ein Routing innerhalb Europas. Wichtig wäre auch, dass wir mehr **Einfluss auf die internationalen Standardisierungsverfahren** gewinnen, denn da mischt die NSA kräftig mit.“ Im Übrigen sei es zu einseitig, jetzt nur eine Bedrohung durch US-amerikanische und britische Dienste an die Wand zu malen, denn russische und chinesische Dienste würden sich im Internet genauso tummeln und Kriminelle sowieso. Insofern seien **Datenschutz und Datensicherheit** unabhängig von der NSA-Affäre das **Gebot der Stunde**.

Die unter dem Schlagwort „**Big Data**“ (vgl. Kapitel 1.2, S. 15 ff.) propagierte Sammlung und Auswertung großer Datenmengen macht nach den Worten des Datenschutzbeauftragten deutlich, dass Daten zunehmend zum **Rohstoff des 21. Jahrhunderts** werden, an dem viele partizipieren wollen: „Das Thema ist mehr als ein aktueller ‚Hype‘. Im Grunde wird hier die gleiche Methode wie bei den Geheimdiensten angewandt: Datenberge werden angelegt und nach Mustern durchsucht, die Computer lernen dazu und sollen am Ende komplexe Prozesse selbsttätig steuern.“

Nach Einschätzung des Landesbeauftragten wird dem Geschäftsmodell Big Data aber nur dann dauerhafter Erfolg beschieden sein, wenn die erhobenen personenbezogenen Daten wirksam anonymisiert werden und keine Rückschlüsse auf Personen mehr möglich sind. Andernfalls drohten Missbrauch und Kontrollverlust. Der Datenschutz müsse von Anfang an eingebaut werden (sog. **privacy by design**); hierfür sei noch viel konzeptionelle Arbeit zu leisten.

Ein künftiger Anwendungsbereich für Big Data wird nach Ansicht des Landesdatenschutzbeauftragten der **Verkehr** sein (vgl. Kapitel 6.1, S. 84 ff.): „Die Industrie rüstet bereits kräftig auf. Ab dem nächsten Jahr soll der von der EU vorgegebene automatische Notruf (e-Call) in den Fahrzeugen Einzug halten. Damit wird ein Einfallstor für weitere Telematikanwendungen geschaffen; hierfür gibt es schon zahlreiche Ideen. Die intelligenten Autos sollen untereinander, mit den Herstellerfirmen, den Werkstätten, anderen Dienstleistern und der Straßeninfrastruktur, auch über das Internet, vernetzt werden. Ohne personenbeziehbare Daten wird das kaum gehen; damit droht uns bald der gläserne Autofahrer. Von tauglichen Datenschutzkonzepten und einer tragfähigen Rechtsgrundlage ist aber weit und breit noch nichts zu sehen! Diese muss nun alsbald geschaffen werden, sonst gerät der Datenschutz im wahrsten Sinne des Wortes unter die Räder.“ Jörg Klingbeil kündigte an, dass sich seine Dienststelle auch in Zukunft mit diesem für Baden-Württemberg wichtigen Thema verstärkt befassen werde.

Neben diesen eher übergreifenden Themen hat seine Dienststelle, so Jörg Klingbeil, im Berichtszeitraum auch zahlreiche Gesetzgebungsvorhaben und Projekte auf **Landesebene** begleitet: „Einen Schwerpunkt hat – wie immer – die **Innere Sicherheit** (vgl. Kapitel 2, S. 40 ff.) gebildet. Vor allem mehrere **Änderungen des Polizeirechts** (Kapitel 2.1, S. 40 ff.) haben meine Mitarbeiter intensiv beschäftigt. Leider sind nicht alle unsere Vorschläge aufgegriffen worden. Besonders ärgerlich ist aus meiner Sicht, wenn die Regierungsparteien an Regelungen festhalten, die sie - so wie ich - zu Oppositionszeiten selbst kritisiert haben (vgl. Kapitel 2.1.4, S. 44 f.): Weiterhin werden unnötigerweise Tatverdächtige für zwei Jahre unter Generalverdacht gestellt und selbst Bagatelldelikte in den polizeilichen Auskunftssystemen gespeichert. Ansonsten war die Polizei im Berichtszeitraum bekanntlich hauptsächlich mit sich selbst, d. h. der **Polizeistrukturreform**, beschäftigt, die meine Dienststelle im Hinblick auf das sog. **Interessenbekundungsverfahren** intensiv begleitet hat (Kapitel 2.3, S. 58 f.).“ Ein permanentes Ärgernis besteht nach Meinung von Jörg Klingbeil im **Verfassungsschutzrecht**: Die verfassungswidrigen Regelungen zum großen Lauschangriff seien auch fast zehn Jahre nach der maßgeblichen Entscheidung des

Bundesverfassungsgerichts immer noch nicht nachgebessert (Kapitel 2.4.1, S. 61 f.); die Landesregierung habe selbst eingeräumt, dass keine entsprechenden Maßnahmen durchgeführt würden. Die Vorschrift könne daher problemlos gestrichen werden.

Gesetzgeberischen Handlungsbedarf sieht der Landesbeauftragte für den Datenschutz auch in Bezug auf die sog. **Zuverlässigkeitsprüfungen**, mit denen sich seine Dienststelle in unterschiedlichen Fallkonstellationen zu befassen hatte (Kapitel 2.2.4, S. 51 ff.). Es geht dabei darum, dass Personen, die Zutritt zu sicherheitsrelevanten Bereichen erhalten oder entsprechende Tätigkeiten ausüben sollen, im Rahmen eines Akkreditierungsverfahrens auf ihre persönliche Zuverlässigkeit mit Hilfe einer Abfrage in polizeilichen, u. U. auch in nachrichtendienstlichen Datenbanken überprüft werden. Da es keine gesetzliche Grundlage hierfür gibt, muss der Betroffene – wenn er Zutritt erlangen oder die Tätigkeit ausüben will – wohl oder übel einwilligen. Im Berichtszeitraum ging es u. a. um die Teilnehmer am Festakt anlässlich der Feierlichkeiten zum Tag der Deutschen Einheit in Stuttgart. Andersgelagerte Fälle betrafen Bewerber für den Polizeivollzugsdienst, Abschleppunternehmer oder Mitarbeiter von Sicherheitsfirmen. „Das Thema begleitet uns seit der Fußballweltmeisterschaft 2006“, erläuterte der Landesdatenschutzbeauftragte, „damals war noch von einer absoluten Ausnahme die Rede. Mittlerweile scheint sich die Zuverlässigkeitsprüfung mit Hilfe einer mehr oder weniger erzwungenen Einwilligung zum Standardinstrument zu entwickeln. Gerade bei Arbeitnehmern kann doch von Freiwilligkeit keine Rede sein. In manchen Fällen, z. B. bei Sicherheitsunternehmen, gibt es überdies gewerberechtliche Zuverlässigkeitsvorschriften zur Genüge; da war es im konkreten Fall völlig verfehlt, das jeweils eingesetzte Personal der Polizei zu melden. Die polizeilichen Dateien sind nicht für diesen Zweck vorgesehen. Es wäre ehrlicher, gesetzlich zu regeln, unter welchen Voraussetzungen die für andere Zwecke vorgesehenen Dateien ebenfalls genutzt werden können. Damit könnte auch den Grundrechten auf Berufsausübung oder auf Pressefreiheit eher Genüge getan werden. Leider lehnen sowohl das Staatsministerium als auch das Innenministerium eine gesetzliche Regelung weiterhin ab.“ Jörg Klingbeil erinnerte in diesem Zusammenhang auch an Querelen um die Zuverlässigkeitsprüfung von Journalisten bei der Leichtathletik-WM 2009 in Berlin.

Ein Aufgabenschwerpunkt war im Berichtszeitraum die **Zusammenarbeit mit den Kommunen** (Kapitel 5.2, S. 78); hierzu Jörg Klingbeil: „Bei unseren Beratungs- und Kontrollbesuchen ist uns wiederholt die Diskrepanz zwischen den datenschutzrechtlichen Anforderungen und der kommunalen Praxis aufgefallen. Mit scharfen Kontrollen und Beanstandungen allein kommt man da nicht weiter. Wir wollen deshalb mit den Kommunalen Landesverbänden und kommunalen Praktikern Handreichungen in

Datenschutzfragen für die kommunale Praxis erarbeiten und haben mit einem Papier zur Veröffentlichung von Fotos durch Kommunen begonnen. Wir unterstützen auch die kommunalen Pilotversuche in Konstanz und Seelbach zur datenschutzkonformen Übertragung von Gemeinderatssitzungen ins Internet. Angesichts der Nachfrage müssen wir hier Lösungen auf der Grundlage des geltenden Rechts finden, also mit informierten Einwilligungen arbeiten, solange es noch keine spezielle gesetzliche Regelung gibt.“

Im Abschnitt **Gesundheit und Soziales** war ein Schwerpunkt erneut die **Orientierungshilfe Krankenhausinformationssysteme** (OH KIS, Kapitel 7.4, S. 97 ff.), die fortgeschrieben und in Zusammenarbeit mit der Baden-Württembergischen Krankenhausgesellschaft und verschiedenen Krankenhäusern konkretisiert und in der Praxis erprobt wurde; sie war im Juni 2013 auch Gegenstand einer gemeinsamen Fachtagung. Die Dienststelle wurde im Berichtszeitraum auch durch zwei gravierende Datenpannen im Krankenhausbereich in Atem gehalten (Kapitel 7.5, S. 100 ff.). Arbeitsschwerpunkte waren außerdem Kontrollen in Pflegeeinrichtungen und in einem Pflegestützpunkt (Kapitel 7.7, S. 104 ff.).

Der wichtige **Datenschutz in Kindertageseinrichtungen** (Kapitel 8.1, S. 115) war Thema einer **Broschüre**, die im September 2012 unter Federführung des Kultusministeriums gemeinsam mit den Kommunalen Landesverbänden und Trägerverbänden, den kirchlichen Datenschutzbeauftragten und der Dienststelle des Landesbeauftragten für den Datenschutz herausgegeben wurde. Der **Datenschutz an Schulen** (Kapitel 8.2., S. 116 ff.) hat nach den Worten des Landesdatenschutzbeauftragten im Berichtszeitraum weitere Fortschritte gemacht: „Das Kultusministerium und meine Dienststelle haben die **Zusammenarbeit** intensiviert. So haben wir bei neuen EDV-Verfahren ebenso mitgewirkt wie bei Fort- oder Ausbildungsmaßnahmen. Aufschlussreich war auch die Kooperation in zahlreichen Einzelfragen mit zwei Schulen im mittleren Neckarraum, von der künftig auch andere Schulen im Land profitieren können. Ein Mitarbeiter meiner Dienststelle hatte auch Gelegenheit, im Beirat für die **Bildungsplanreform 2015** mitzuwirken. Dies ist sinnvoll, denn Datenschutz muss als Teil der Medienkompetenz auch ein prüfungsrelevantes Thema im Unterricht werden, nicht nur mit den technischen, sondern vor allem mit den wertegebundenen Aspekten. Bisher passiert in dieser Richtung noch zu wenig.“ Lobenswert war nach Ansicht des Landesdatenschutzbeauftragten dagegen das vom Kultusministerium im Sommer 2013 für Schulen ausgesprochene **Verbot der dienstlichen Kommunikation über Soziale Netzwerke** (Kapitel 8.2.7, S. 120 f.). Einen datenschutzrechtlichen Konflikt sieht Jörg Klingbeil bei der geplanten **Einführung einer landeseinheitlichen Bil-**

bildungsnummer heraufziehen (Kapitel 8.2.8, S. 121 f.): „Nach derzeitigem Stand halte ich eine landeseinheitliche und permanente Bildungsnummer für Schüler, um die Schulverwaltung zu vereinfachen oder Statistiken für Bildungsverläufe zu ermöglichen, nicht für erforderlich. Generell sind zentrale Datenbestände aus Sicht des Datenschutzes immer mit größeren Risiken verbunden als dezentrale Strukturen.“

Ungeachtet der Tatsache, dass nach wie vor die überfällige Neuregelung des Beschäftigtendatenschutzes aussteht (Kapitel 1.4.1, S. 28 f.), ist der **Datenschutz in der Arbeitswelt** (Kapitel 9, S. 126 ff.) weiterhin ein Beratungsschwerpunkt der Dienststelle des Landesbeauftragten für den Datenschutz. Im Tätigkeitsbericht werden als Einzelthemen behandelt:

- Alkoholtests am Arbeitsplatz,
- Einholung von Auskünften bei früheren Arbeitgebern,
- zulässiger Inhalt von Personalakten.

Der **Datenschutz in der Wirtschaft** (Kapitel 10, S. 129 ff.) ist im Tätigkeitsbericht mit etlichen Einzeldarstellungen vertreten. So wird u. a. den Fragen nachgegangen, ob einem betrieblichen Datenschutzbeauftragten im Insolvenzverfahren gekündigt werden kann (Kapitel 10.1, S. 129 f.), wie Werbung und Datenschutzerklärungen im Internet datenschutzkonform gestaltet werden können (Kapitel 10.2 bis 10.4, S. 131 ff.) oder welche personenbezogenen Abrechnungsdaten ein Hausverwalter wie weiterleiten darf (Kapitel 10.7, S. 144). Ein weiterer Themenschwerpunkt sind erneut die rechtlichen Schranken für die Tätigkeit von Wirtschaftsauskunfteien (Kapitel 10.8-11, S. 145 ff.).

Der Abschnitt **Technik und Medien** (Kapitel 11, S. 150 ff.) spiegelt mit dem Thema **Videoüberwachung** (Kapitel 11.1, S. 150 ff.) einen besonders arbeitsintensiven Aufgabenbereich des Landesbeauftragten für den Datenschutz wider; hierzu Jörg Klingbeil: „Videoüberwachungsanlagen haben sich zum echten Dauerbrenner bei den vielfältigen Beschwerden der Bürgerinnen und Bürger entwickelt und sind zu einer Jedermann-Technik, weil technisch ausgereift und preiswert, geworden. Ein besonderes Ärgernis sind die sog. **Wildkameras** (Kapitel 11.1.4, S. 152 f.), die regelmäßig sogar von Discountern angeboten werden – so viele Jäger und Förster kann es in Deutschland gar nicht geben. Dabei sind Wildkameras im Wald in der Regel unzulässig, weil die berechtigten Interessen der Waldbesucher überwiegen. Der Wald dient der Erholung der Menschen und muss deshalb von Überwachungseinrichtungen frei bleiben.“ Ein weiterer Schwerpunkt des Abschnitts ist das Thema **Cloud Computing** (Kapitel 11.4, S. 162); exemplarisch vertieft wird dabei die Frage, ob Dropbox unbe-

denklich genutzt werden kann (Kapitel 11.4.2, S. 166 f.). Im Hinblick auf das eingangs genannte Risiko, dass US-amerikanische Sicherheitsbehörden ggf. auf die bei **Dropbox** gespeicherten Daten zugreifen können, wird die Verschlüsselung der dort abgelegten Daten mit einem eigenen privaten Schlüssel empfohlen. Der Bericht stellt ferner die neue **DIN-Norm 66399** mit erweiterten Vorgaben zur Datenträgervernichtung vor (Kapitel 11.3, S. 160 ff.).

Im **Anhang** des Berichts werden die **Entschließungen bzw. Beschlüsse** der Datenschutzaufsichtsbehörden des Bundes und der Länder im Berichtszeitraum dokumentiert.

Bei Rückfragen erreichen Sie uns unter der Telefonnummer 0711/615541-0. Weitere Informationen zum Datenschutz finden Sie im Internet unter www.baden-wuerttemberg.datenschutz.de oder unter www.datenschutz.de. Die Pressemitteilung ist im Internet abrufbar unter <http://www.baden-wuerttemberg.datenschutz.de>.