



Baden-Württemberg

DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ

SPERRFRIST: Montag, 12. Dezember 2011, 11 Uhr

PRESSEMITTEILUNG

12. Dezember 2011

** Die Themenpalette reicht nun von Facebook bis „Staats-Trojaner“
Landesbeauftragter für den Datenschutz stellt ersten Tätigkeitsbericht nach der
Zusammenlegung der Aufsichtsbehörden vor**

Der Landesbeauftragte für den Datenschutz, Jörg Klingbeil, hat anlässlich der Vorstellung seines 30. Tätigkeitsberichts am 12. Dezember 2012 in Stuttgart auf die erheblichen Veränderungen durch die Zusammenlegung seiner Dienststelle mit der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich hingewiesen: „Unsere bisherige Themenpalette hat sich seit dem 1. April 2011 deutlich erweitert. Wenn man die dominierenden Themen der letzten Wochen betrachtet, dann kann die jetzige Bandbreite am besten mit den Stichworten Facebook und ‚Staats-Trojaner‘ umschrieben werden.“ Umfangreiche Synergieeffekte seien bislang allerdings ausgeblieben; dazu seien die datenschutzrechtlich zu beurteilenden Sachverhalte und Institutionen – auf der einen Seite Behörden, auf der anderen Seite Unternehmen – doch zu unterschiedlich. Für den Bürger dürfte im Alltag allerdings der Datenschutz im nicht-öffentlichen Bereich zumeist die größere Rolle spielen, sei es als Kunde an der Ladenkasse oder bei Bestellungen über das Internet, als Opfer unerwünschter Werbung oder als Bewertungsobjekt undurchsichtiger Scoringverfahren und vor allem immer wieder als Arbeitnehmer. „Einigendes Band“ vieler datenschutzrechtlicher Fragestellungen seien die eingesetzten technischen Mittel, das heißt die zunehmende „Digitalisierung des Alltags“ und die Durchdringung vieler Lebenswirklichkeiten durch das Internet, ergänzte der Landesdatenschutzbeauftragte. Das „Internet der Dinge“ stehe vor der Tür. Stichworte seien die sog. intelligenten Stromzähler, der Einsatz des Internets in Fahrzeugen, die weitere Verbreitung von Ortungstechnik oder die flexible Auslagerung der Datenverarbeitung in verschiedene Rechenzentren (Cloud Computing). Die Datenspuren würden immer zahlreicher; mit der allgegenwärtigen Datenverarbeitung wachse auch die Gefahr, dass von interessierten Stellen – seien sie staatlich oder wirtschaftlich motiviert – persönliche Nutzungsprofile ausgewertet werden können und das Recht auf informationelle Selbstbestimmung auf der Strecke bleibt. Das Datenschutzrecht halte damit kaum Schritt und sei zunehmend

modernisierungsbedürftig. Insofern setze er eine gewisse Hoffnung in die bevorstehende grundlegende Überarbeitung des europäischen Rechtsrahmens.

„Nach wie vor habe ich den Eindruck, dass viele Menschen mit der technischen Entwicklung kaum mitkommen und vom Web 2.0 überfordert sind. Wer weiß denn schon, was mit den Nachrichten oder Bildern passiert, die er selbst oder Freunde auf sozialen Netzwerken veröffentlichen? Zu viele gehen mit ihren Daten zu sorglos um. Diese Sorglosigkeit betrifft aber nicht nur das private Umfeld, das fehlende Bewusstsein für Datenschutz und Datensicherheit scheint sich auch auf das berufliche Umfeld zu übertragen. Umfragen zeigen, dass viele Unternehmen das Thema IT-Sicherheit stark vernachlässigen. Schwachpunkte sind dabei die unzureichende Regelung von Zugriffsrechten und der Umgang mit E-Mails und mobilen Geräten, die häufig sensible Daten des Unternehmens enthalten. Das ist besonders fatal, weil bereits die Hälfte aller deutschen Unternehmen mittelmäßig bis stark vom Internet abhängen“, erläuterte der Landesdatenschutzbeauftragte.

Zu einzelnen Themenschwerpunkten des Berichts teilte der Landesdatenschutzbeauftragte Folgendes mit:

Die bis zum April 2011 in wenigen Fällen durchgeführte sog. Quellen-Telekommunikationsüberwachung sei mit erheblichen Mängeln behaftet gewesen. „Die vom Chaos Computer Club an einer Variante der Software festgestellten Mängel haben sich bei unserer Kontrolle im Landeskriminalamt im Wesentlichen bestätigt. Der Hauptfehler lag nach unserem Eindruck darin, dass die Ermittlungsbehörden der angemieteten Software und den Anpassungsarbeiten der Softwarefirma vertrauten, ohne selbst alle Funktionalitäten zu überblicken. Diese Art von Outsourcing in einem Kernbereich hoheitlichen Handelns sollte künftig unterbleiben. Außerdem halte ich es für einen schweren Fehlgriff, bei den Abhörmaßnahmen Gerätschaften außerhalb Europas, im konkreten Fall einen Server in den USA, einzusetzen,“ kommentierte der Landesbeauftragte die Ergebnisse der Kontrolle. Wenn künftig eigene staatliche Kompetenzen für die Durchführung der Maßnahme aufgebaut würden und über eine Präzisierung der gesetzlichen Regelungen nachgedacht werde, dann sei das aus Sicht des Datenschutzes zu begrüßen. Bis dahin dürfe aber keine Quellen-TKÜ mehr durchgeführt werden (siehe hierzu Anlage 1).

Im Sicherheitsbereich gebe es auch andere Entwicklungen, die Sorge bereiteten, erklärte Jörg Klingbeil. „In Europa werden, nahezu unbemerkt von der Öffentlichkeit, mit öffentlichen Fördermitteln zahlreiche Forschungsvorhaben vorangetrieben, die

‚verdächtiges‘ Verhalten erkennen sollen. Das bedenklichste Beispiel ist das von der EU-Kommission geförderte Projekt INDECT, ein umfassendes Überwachungssystem, das dem Vernehmen nach erstmals bei der Fußball-Europameisterschaft im nächsten Jahr getestet werden soll. Es vernetzt Überwachungskameras, Gesichtserkennungssoftware, Drohnen und Online-Recherchen, alles mit dem Ziel, das Leben sicherer zu machen. Diese Totalüberwachung wäre in Deutschland glatt verfassungswidrig. INDECT scheint sich eher für Diktaturen zu eignen,“ kritisierte der Landesdatenschutzbeauftragte. Auch im Lande werde an ähnlicher Überwachungssoftware geforscht. Dies habe sich im Sommer 2011 gezeigt, als der geplante Test des Projekts PaGeVi („Parallele Gesichtserkennung in Videoströmen“) des KIT im Karlsruher Wildparkstadion in letzter Minute gestoppt wurde. Sinnvoller erscheine demgegenüber der interdisziplinäre Ansatz des Tübinger Projekts MuViT („Mustererkennung und Video Tracking“), das ethische und verfassungsrechtliche Perspektiven einbeziehe; auf die Ergebnisse sei er gespannt (siehe hierzu Anlage 2).

Unabhängig von diesen eher spektakulären Projekten sei die Zusammenarbeit seiner Dienststelle mit der Polizei von dem gemeinsamen Bemühen um eine kontinuierliche Qualitätsverbesserung der polizeilichen Datenverarbeitung geprägt, ergänzte Jörg Klingbeil. „Wir sind zwar nicht immer einer Meinung, stehen aber in einem permanenten Erfahrungs- und Meinungsaustausch. Manche Webfehler der Vergangenheit können allerdings nicht im Verwaltungsvollzug wettgemacht, sondern müssen durch den Gesetzgeber ausgebessert werden, zum Beispiel hinsichtlich der Speicherung von Bagatelldelikten oder was die sogenannte Prüffallregelung angeht.“ Eine Qualitätsverbesserung bedinge aber auch eine vernünftige Personalausstattung der Datenstationen in den Polizeidirektionen und ein durch intensive Aus- und Fortbildung zu steigendes Datenschutzbewusstsein auf der Sachbearbeiterbene.

Welche merkwürdigen Blüten der Wunsch nach umfassender Sicherheit treibt, lasse sich nach den Worten von Jörg Klingbeil gut am Beispiel der sogenannten Antiterrorlisten von EU und UN beobachten. Viele Unternehmen würden mittlerweile die Daten ihrer Mitarbeiter und Kunden mit diesen, nach den Anschlägen vom 11. September 2001 entstandenen Listen anlasslos und umfassend abgleichen, ohne dass der Nutzen erkennbar sei. „Bei uns sind in letzter Zeit sogar einige Beschwerden von Bankkunden eingegangen, die sich beim Umtausch von Devisen in relativ geringem Umfang ausweisen mussten, damit ihre Daten mit den Antiterrorlisten abgeglichen werden konnten,“ erläuterte der Landesdatenschutzbeauftragte den ärgerlichen Befund (siehe hierzu Anlage 3).

Einen gewissen Kontrollschwerpunkt hat im Berichtszeitraum der Gesundheitsbereich gespielt. Die umfangreiche Kontrolle eines großen Klinikums förderte erhebliche Mängel im Krankenhausarchiv und bei der Videoüberwachung zutage, erläuterte Jörg Klingbeil. „Mitursächlich für die festgestellten Mängel war unseres Erachtens der Umstand, dass der arme Datenschutzbeauftragte des Klinikums völlig auf sich allein gestellt war und außerdem noch andere Aufgaben zu erledigen hatte. Das ist gerade in einem Bereich, in dem besonders sensible Daten verarbeitet werden, ein völlig unhaltbarer Zustand. Bezeichnend war zudem, dass dem Datenschutzbeauftragten die einzelnen Videoüberwachungsmaßnahmen gar nicht erst gemeldet wurden.“ (siehe hierzu Anlage 4).

Erheblichen Raum nimmt im 30. Tätigkeitsbericht das Thema „Datenschutz in der Arbeitswelt“ ein. „In unserer Beratungspraxis merken wir, dass dieses Thema immer wichtiger wird. Ein Großteil der Fragen betrifft das Fragerecht des Arbeitgebers im Rahmen von Bewerbergesprächen. Hier werden wir weiterhin für einen restriktiven Kurs eintreten,“ kündigt Klingbeil an (siehe hierzu Anlage 5).

Die Digitalisierung des Alltags greift nach Meinung des Landesbeauftragten für den Datenschutz immer weiter um sich. Gerade für junge Menschen sind Computer und Internet schon absolute Selbstverständlichkeiten geworden. Die Nutzungshäufigkeit und Verweildauer nehmen dabei zu. Insbesondere die sozialen Netzwerke haben eine erhebliche Bindungswirkung. Vier Fünftel aller Jugendlichen nutzen diese Plattformen regelmäßig, wobei der amerikanische Anbieter Facebook mittlerweile seine deutschen Mitbewerber in der Gunst der Nutzer deutlich überrundet hat. Erfreulicherweise scheinen die Jugendlichen hinsichtlich des Umgangs mit den eigenen oder fremden Daten in sozialen Netzwerken mittlerweile sensibler geworden zu sein, erklärte der Landesdatenschutzbeauftragte. Dies zeige die jüngste JIM-Studie (2011): Der Anteil derer, die ihr Profil mit einer Privatsphäre-Einstellung vor den Einblicken Dritter geschützt haben, sei von 67 % in 2010 auf 79 % in 2011 gestiegen. Dieser grundsätzlich erfreuliche Befund werde allerdings durch die große Zahl der „Freunde“ in sozialen Netzwerken (Durchschnitt: 200 Personen) stark relativiert. Hierzu der Landesbeauftragte: „Von einer echten Privatsphäre kann angesichts dieser Zahlen kaum die Rede sein. Die Grenzen zwischen öffentlich und privat verschwimmen zusehends. Hier zeigt sich auch das grundlegende Dilemma der sozialen Netzwerke aus der Sicht der Jugendlichen: Geben sie zu wenig von sich preis, sind sie für andere uninteressant und erfahren auch von diesen wenig; offenbaren sie hingegen zu viel Persönliches, kann mit diesen Daten Missbrauch getrieben werden.“ Es sei höchste Zeit, dass sich die international tätigen sozialen

Netzwerke an das deutsche und das europäische Datenschutzrecht hielten und vor allem nicht die Daten der Nutzer ohne deren Einwilligung einsammelten, meinte Jörg Klingbeil. An die deutschen Betreiber von Webseiten richtete er die Mahnung, mit gutem Beispiel voranzugehen und auf die Einbindung sog. Social Plug-ins in ihre Internetauftritte zu verzichten. Hier sei etwas mehr kritische Distanz angebracht, um Facebook und Co. zu einem Einschwenken auf die deutschen Datenschutzstandards zu bewegen (siehe hierzu Anlage 6).

Abschließend ging der Landesdatenschutzbeauftragte auf die internen Auswirkungen der Zusammenlegung ein: „Die Fusion hat mehr als ein halbes Jahr viel Arbeitskraft gekostet. Bis zu unserem Umzug in neue Diensträume Ende Oktober 2011 war der Dienstbetrieb erheblich beeinträchtigt; nun geht es wieder aufwärts.“ Für einen optimistischen Ausblick in die Zukunft des Datenschutzes in Baden-Württemberg habe auch die neue Landesregierung gesorgt, die in ihrer Koalitionsvereinbarung eine Stärkung des unabhängigen Datenschutzes versprochen habe. „Jetzt wird es allmählich Zeit, dass den schönen Worten auch Taten folgen“, meinte Jörg Klingbeil mit Blick auf die bevorstehenden Haushaltsverhandlungen, „im Vergleich zu den Datenschutzaufsichtsbehörden in anderen Bundesländern haben wir immer noch Nachholbedarf.“

Der Tätigkeitsbericht ist ab 12. Dezember 2011, 11.00 Uhr, im Internet unter der Adresse <http://www.baden-wuerttemberg.datenschutz.de> abrufbar.

Zu folgenden Themen sind jeweils nähere Informationen angeschlossen:

1. Landesbeauftragter für den Datenschutz:
Einsatz des „Staats-Trojaners“ war mangelhaft; kein „Outsourcing“ im Kernbereich hoheitlichen Handelns.
2. Sicherheitsforschung als Handlanger für Diktaturen?
3. Landesbeauftragter für den Datenschutz:
Devisentausch nur noch mit Identitätsnachweis?
Kein systematischer, anlassloser Abgleich von Arbeitnehmer- und Kundendaten mit den sogenannten Antiterrorlisten
4. Das datenschutzkranken Klinikum
5. Landesbeauftragter für den Datenschutz:
Datenschutz in der Arbeitswelt wird immer wichtiger.
6. Soziale Netzwerke müssen das deutsche Datenschutzrecht beachten.
Landesbeauftragter mahnt Behörden zur Zurückhaltung bei der Einbindung des sog. Gefällt-mir-Buttons von Facebook auf ihren Internetseiten.

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 www.baden-wuerttemberg.datenschutz.de/afd/pm/default.htm.

Sperrfrist: Montag, 12. Dez. 2011, 11 Uhr



Baden-Württemberg

DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ

Anlage 1 zur Pressemitteilung vom 12. Dezember 2011

Sperrfrist: 12. Dezember 2011, 11 Uhr

Landesbeauftragter für den Datenschutz:

Einsatz des „Staats-Trojaners“ war mangelhaft; kein „Outsourcing“ im Kernbereich hoheitlichen Handelns

(S. 46 ff.)

Der Einsatz des sog. Staats-Trojaners durch baden-württembergische Ermittlungsbehörden war mangelhaft. Dies gab der Landesbeauftragte für den Datenschutz, Jörg Klingbeil, anlässlich der Vorstellung seines Tätigkeitsberichts am 12. Dezember 2011 in Stuttgart bekannt. „Wie unser Kontrollbesuch im Landeskriminalamt ergeben hat, war der Hauptmangel, dass die Behörden keine vertieften Kenntnisse über die Möglichkeiten der angemieteten Erfassungssoftware hatten. Es reicht nicht aus, dass sich das Landeskriminalamt auf die Zusicherungen der Softwarefirma verlässt und die bestellten Voreinstellungen auf ihre Vereinbarkeit mit den richterlichen Anordnungen testet. Hierdurch kann man nicht die tatsächlich vorhandenen Funktionalitäten einer Software feststellen. Es ist höchste Zeit, dass die staatlichen Stellen wieder Herr des Verfahrens werden. Außerdem halte ich es für einen schweren Fehlgriff, wenn die Telekommunikationsüberwachung unter Verwendung von Rechnern außerhalb Europas durchgeführt wird.“ Das Landeskriminalamt hatte zur Legendierung einen Server in den USA eingesetzt.

Eine Variante des „Staats-Trojaners“ war durch den Chaos Computer Club (CCC) Anfang Oktober 2011 eingehend analysiert worden. Dabei hatten sich einige Schwachstellen gezeigt, die sich bei der anschließenden Kontrolle der in Baden-Württemberg eingesetzten Software durch die Dienststelle des Landesbeauftragten bestätigten. Jörg Klingbeil hierzu: „Die Vorarbeit des CCC war ausgesprochen hilfreich. Dabei will ich nicht die Quellen-Telekommunikationsüberwachung (Quellen-TKÜ), also die Infiltration des Computers einer Zielperson, um aus- oder eingehende Telefonate vor bzw. nach der Verschlüsselung zu überwachen, grundsätzlich in Frage stellen.“ Eine solche Maßnahme könne wegen der zunehmenden Verbreitung von

verschlüsselter Internet-Telefonie unter engen Voraussetzungen zulässig sein. Sie müsse aber wegen der schwierigen Abgrenzung zur Online-Überwachung und wegen des u. U. tangierten Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme mit höchster Präzision durchgeführt werden. Nur dann könne die Quellen-TKÜ datenschutzrechtlich zulässig durchgeführt werden. Daran habe es auch in Baden-Württemberg gefehlt. Weder hätten die Gesprächspartner des Landeskriminalamtes zu den in der Presse berichteten Schwächen der Verschlüsselung noch zur Authentisierung der Fernsteuerung der Erfassungssoftware brauchbare Angaben machen können. Das Sicherheitsproblem, dass Dritte infolge der Nachladefunktion Programme und Daten hätten nachladen können, sei entweder nicht erkannt oder nicht entschieden genug angegangen worden. „Ganz offensichtlich war die Kontrolle des Unternehmens nicht hinreichend“, erklärte Jörg Klingbeil. „Ich halte ein derartiges Outsourcing im Kernbereich hoheitlichen Handelns für nicht länger tragbar. In Zukunft werden die Ermittlungsbehörden anhand des Quellcodes selber prüfen müssen, was die Überwachungssoftware wirklich kann.“

Der Umstand, dass die Quellen-TKÜ im Zeitraum bis April 2011 von baden-württembergischen Ermittlungsbehörden nur vier Mal durchgeführt wurde und dass die Abhörmaßnahmen durch den derzeitigen baden-württembergischen Innenminister vorerst gestoppt wurden, ist nach den Worten des Landesbeauftragten dabei ein schwacher Trost. Denn schon werde von Sicherheitspolitikern eine Schutzlücke an die Wand gemalt und gefordert, die unterbrochenen Maßnahmen alsbald wieder fortzusetzen. Hierzu Jörg Klingbeil: „Nun müssen zunächst die Hausaufgaben gemacht und die bisherigen Defizite beseitigt werden; erst dann kann es weitergehen. Die jüngsten Überlegungen, ein Kompetenzzentrum für die Quellen-TKÜ auf Bundesebene aufzubauen und künftig eine Überprüfung des Quellcodes zu ermöglichen, weisen in die richtige Richtung. Aber auch der Gesetzgeber ist nun gefordert, die rechtlichen Voraussetzungen für eine Quellen-TKÜ präziser zu regeln.“



Baden-Württemberg

DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ

Anlage 2 zur Pressemitteilung vom 12. Dezember 2011

Sperrfrist: 12. Dezember 2011, 11 Uhr

Sicherheitsforschung als Handlanger für Diktaturen?

(S. 135 ff.)

Kriminalität, Katastrophen, Gewalt bei Großveranstaltungen – die Liste der denkbaren Risiken in unserer Gesellschaft ist lang. „Ebenso groß ist aber offensichtlich der Ehrgeiz, Risiken möglichst frühzeitig zu erkennen, um das Sicherheitsbedürfnis der Bevölkerung zu befriedigen“, erklärte der Landesbeauftragte für den Datenschutz, Jörg Klingbeil, anlässlich der Vorstellung seines Tätigkeitsberichts am 12. Dezember 2011 in Stuttgart. „Fast unbemerkt von der Öffentlichkeit sind in den letzten Jahren zahlreiche Forschungsprojekte entstanden, die sich schwerpunktmäßig der Erkennung ‚verdächtigen‘ Verhaltens widmen. Neben dem seit 2007 bestehenden Programm der Bundesregierung zur Sicherheitsforschung, für das 235 Mio. Euro bis Ende des Jahres 2013 bereitgestellt worden sind und das auch mehrere Forschungsvorhaben in Baden-Württemberg fördert, gibt es auf europäischer Ebene das umstrittene Projekt INDECT, das möglicherweise bei der Fußball-Europameisterschaft 2012 in Polen und der Ukraine zum ersten Mal getestet wird – offenbar auch an Zuschauern aus unserem Land. Die mit INDECT beabsichtigte Totalüberwachung wäre in Deutschland eindeutig verfassungswidrig. Soweit deutsche Stellen derartige Forschungen unterstützen oder selbst betreiben, stellt sich massiv die Frage, wo eine derartige Technik später eingesetzt werden soll. Die Sicherheitsforschung darf keine Handlangerdienste für Diktaturen leisten. Bezogen auf Europa muss die Frage gestattet sein, welche gemeinsamen Wertvorstellungen eigentlich in Europa bestehen.“

Insofern sei es nur zu begrüßen, meinte der Landesdatenschutzbeauftragte, dass sich das von der EU-Kommission geförderte Projekt INDECT im Europäischen Parlament zunehmend kritischen Fragen ausgesetzt sehe. INDECT vernetze verschiedene Überwachungsmittel wie Kameras, Drohnen, Gesichtserkennungssoftware, Online-Analyse und verschiedene Computersysteme zu einem großen Sicherheitssystem, das „abnormales“ Verhalten frühzeitig erkennen solle. Das könne nach Ein-

schätzung der hierzu befragten Polizeibeamten und Sicherheitsdienste „Herumlungern“ ebenso sein wie „schnelles Laufen“, „langes Betrachten eines Kraftfahrzeugs“, „Geschrei“ oder ein „plötzlicher Richtungswechsel“.

Aber auch in Deutschland gibt es nach den Worten des Landesdatenschutzbeauftragten einige öffentlich geförderte Forschungsprojekte, die sich der Erkennung „verdächtigen“ Verhaltens widmen. So zum Beispiel das im Sommer 2011 in die Schlagzeilen geratene Projekt „PaGeVi“ („Parallele Gesichtserkennung in Videoströmen“) des Karlsruher Instituts für Technologie (KIT), das in Zusammenarbeit mit einer Sicherheitsfirma betrieben worden sei. „Das Institut wollte – worauf mich die Medien, mehrere Bürger und Fußball-Fanclubs hinwiesen – bei einem Fußballspiel des Karlsruher SC mit Videokameras testen, ob bestimmte Testpersonen in einer Menschenmenge wiedererkannt werden. Dass dabei auch Unbeteiligte ins Visier geraten könnten, schien vorher niemanden zu stören“, erläuterte Jörg Klingbeil. „Allerdings war nach meinen Recherchen außer den Projektverantwortlichen offiziell niemand in die Überlegungen eingeweiht. Die Vereinsspitze, die Stadt, das Polizeipräsidium und natürlich die Fans des KSC waren ahnungslos. Selbst die Datenschutzbeauftragten der Universität wussten von nichts.“ Insofern sei es vernünftig gewesen, den Feldversuch umgehend zu stoppen und das weitere Vorgehen noch einmal kritisch zu überprüfen.

Demgegenüber sei der breite Forschungsansatz des Projekts MuViT („Mustererkennung und Video Tracking“) zu begrüßen, bei dem das Internationale Zentrum für Ethik in den Wissenschaften der Universität Tübingen in Zusammenarbeit mit weiteren drei deutschen Universitäten interdisziplinär sozialpsychologische, soziologische, ethische und rechtswissenschaftliche Analysen erarbeiten und Lösungen anbieten will. „Ich bin auf die Forschungsergebnisse schon sehr gespannt“, meinte Jörg Klingbeil abschließend, „weil das Projekt im Vorfeld einer technischen Umsetzung die erforderliche ethische Orientierung und verfassungsrechtliche Einordnung bieten kann. Dass Technik viel kann und immer leistungsfähiger wird, ist unbestritten. Die entscheidende Frage wird aber sein, ob wir alles realisieren sollen, was technisch machbar ist. Ich erinnere auch daran, dass es nach der Rechtsprechung des Bundesverfassungsgerichts zur verfassungsrechtlichen Identität Deutschlands gehört, dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf. Wenn ich mich im öffentlichen Raum nicht mehr unbeobachtet bewegen kann, ist die verfassungsrechtliche Schmerzgrenze überschritten“.



Baden-Württemberg

DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ

Anlage 3 zur Pressemitteilung vom 12. Dezember 2011

Sperrfrist: 12. Dezember 2011, 11 Uhr

Landesbeauftragter für den Datenschutz:

Devisentausch nur noch mit Identitätsnachweis?

Kein systematischer, anlassloser Abgleich von Arbeitnehmer- und Kundendaten mit den sogenannten Antiterrorlisten

(S. 230 ff., S. 286 ff.)

„Wer für einen Kurzurlaub im Ausland Devisen bei seiner Bank umtauschen will, läuft Gefahr, dass sein Name mit den hochproblematischen Antiterrorlisten abgeglichen wird.“ Auf diesen Befund hat der Landesbeauftragte für den Datenschutz, Jörg Klingbeil, anlässlich der Vorstellung seines Tätigkeitsberichts am 12. Dezember 2011 in Stuttgart hingewiesen. „Mehrere Bürger haben sich bei mir darüber beschwert, dass Kreditinstitute die Vorlage des Personalausweises verlangten, auch wenn die Betroffenen nur ein paar Hundert Schweizer Franken für einen Kurzurlaub in der Schweiz umtauschen wollten.“ Als Begründung sei selbst bei Gelegenheitskunden angegeben worden, dass die erhobenen Daten mit den sogenannten Antiterrorlisten abgeglichen und zu Revisionszwecken gespeichert werden müssten.

Zum Hintergrund erläuterte der Landesbeauftragte, dass die sogenannten Antiterrorlisten der EU und der Vereinten Nationen nach den Anschlägen vom 11. September 2001 geschaffen wurden, um eine wirtschaftliche Unterstützung von Terroristen und terrorverdächtigen Organisationen oder Personen zu verhindern. Wer auf diesen Listen geführt wird, dürfe weder Geld noch sonstige wirtschaftliche Ressourcen erhalten. Das betreffe auch die eigenen Mitarbeiter. Das umfassende Verbot richte sich sowohl an staatliche Stellen wie auch an Unternehmen. Hierzu Jörg Klingbeil: „Das Verbot hat mittlerweile absurde Folgen: Viele Unternehmen fühlen sich genötigt, die Personalien ihrer Mitarbeiter und Kunden flächendeckend mit den Antiterrorlisten abzugleichen, obwohl keinerlei Verdacht einer Zugehörigkeit zu terroristischen Gruppierungen besteht.“ Dabei sei nach wie vor umstritten, ob die Antiterrorlisten überhaupt einen nennenswerten Beitrag zur Verhinderung einschlägiger Straftaten leisten könnten.

Zwar habe sich die Lage etwas verbessert, weil die Betroffenen mittlerweile von der EU-Kommission über ihre Aufnahme in die Listen unterrichtet werden müssen und hierzu auch eine Gegenäußerung abgeben können, die dann dem Sanktionsausschuss der Vereinten Nationen zugeleitet wird. Was dort damit geschieht, sei aber von hier aus ebenso schwer zu beurteilen wie die Frage, wie man überhaupt auf die Listen geraten kann.

Der Landesbeauftragte für den Datenschutz hält das ganze Verfahren für hochproblematisch: „Kunden und Mitarbeiter von Unternehmen dürfen nicht unter einen Generalverdacht terroristischer Aktivitäten gestellt werden. Ein flächendeckender, systematischer und anlassloser Abgleich von Mitarbeiter- und Kundendaten mit den Antiterrorlisten hat daher zu unterbleiben. Soweit Kundendaten allein für einen unzulässigen Datenabgleich erhoben worden sind, kommt auch ihre Speicherung nicht in Betracht.“

Abschließend wies Jörg Klingbeil darauf hin, dass die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich („Düsseldorfer Kreis“) bereits im Jahr 2009 einen Abgleich von Mitarbeiterdaten mit Antiterrorlisten durch Unternehmen für unzulässig gehalten hatten, weil es für die Listen keine belastbare Rechtsgrundlage gibt; die EU-Verordnungen genügten nämlich nicht dem rechtsstaatlichen Bestimmtheitsgebot. Auch bestünden Zweifel an der Rechtsstaatlichkeit des Zustandekommens der Listen und immer noch unzureichende Rechtsschutzmöglichkeiten.

Die Bundesregierung teilt diese Zweifel. Nach einer Mitteilung des Auswärtigen Amtes sind Unternehmen und andere Wirtschaftsbeteiligte nicht zu einem systematischen anlassunabhängigen Abgleich ihrer Kunden- und Mitarbeiterdaten verpflichtet. Aufgrund des verfassungsrechtlichen Verhältnismäßigkeitsgrundsatzes könne eine solche Verpflichtung nur bestehen, wenn die jeweils geltenden Sorgfaltspflichten ein entsprechendes Vorgehen notwendig machen.

Über die Einzelheiten der von den Unternehmen anzuwendenden Sorgfaltsmaßstäbe herrsche nach den Erfahrungen der Aufsichtsbehörden aber nach wie vor Unklarheit, ergänzt der Landesbeauftragte. Feststehen dürfte jedoch, dass ein Datenabgleich nur in Betracht kommt, wenn ein konkreter Verdacht vorliegt, dass der betroffene Mitarbeiter oder Kunde zu dem Personenkreis gehört, der in den Antiterrorlisten aufgeführt ist. Jörg Klingbeil abschließend: „Die Rechtsschutzmöglichkeiten gegen eine Aufnahme in die Antiterrorliste müssen auf internationaler Ebene verbessert werden. Bis es soweit ist, sind Abgleiche von Mitarbeiter- und Kundendaten restriktiv zu handhaben.“



Baden-Württemberg

DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ

Anlage 4 zur Pressemitteilung vom 12. Dezember 2011

Sperrfrist: 12. Dezember 2011, 11 Uhr

Das datenschutzkranke Klinikum

(S. 141 ff.)

„Patientinnen und Patienten erwarten im Krankenhaus nicht nur eine optimale Gesundheitsversorgung, sondern auch einen verantwortungsvollen Umgang mit ihren Daten. Für den Umgang mit diesen Daten gibt es Regeln, die von Krankenhausmitarbeitern und -verwaltung sorgfältig zu beachten sind“, erklärte der Landesbeauftragte für den Datenschutz, Jörg Klingbeil, anlässlich der Vorstellung seines Tätigkeitsberichts am 12. Dezember 2011 in Stuttgart.

Dass dies in der Krankenhausrealität leider nicht immer der Fall sei, habe einmal mehr ein Kontrollbesuch eines großen Klinikums in Baden-Württemberg bestätigt. Zwar herrsche in wichtigen Bereichen wie Patientenaufnahme, Verwaltung, Krankenhausapotheke, aber auch auf den Krankenstationen ein hohes Datenschutzbewusstsein. Dem stünden allerdings schwerwiegende Datenschutzmängel im Krankenhausarchiv und bei den vom Krankenhaus betriebenen Videoüberwachungsanlagen gegenüber.

„Geradezu erschreckend war für mich der überaus sorglose Umgang der Beschäftigten des Archivs mit den dort aufbewahrten Patientenakten“, fuhr Klingbeil fort. Existierende archivrechtliche Vorschriften seien weder bekannt gewesen noch beachtet worden. Dies habe u. a. dazu geführt, dass nicht verlässlich nachvollzogen werden konnte, wo sich Patientenakten oder Teile davon befinden und wer diese wann und zu welchen Zwecken dem Archiv entnommen habe. Fehlende Zugangskontrollen ermöglichten zudem ohne Weiteres Aktenentnahmen außerhalb der üblichen Öffnungszeiten, Patientendaten seien eher zufällig als planmäßig vernichtet bzw. gelöscht worden. Das Klinikum habe sich einsichtig gezeigt und die Archivordnung um die wichtigsten Bestimmungen zur Archivierung von Patientenakten ergänzt. „Jetzt muss das Klinikum dafür sorgen, dass die Archivmitarbeiterinnen und -mitarbeiter regelmäßig

geschult werden und der datenschutzkonforme Umgang mit Patientendaten kontrolliert wird“, appellierte der Landesdatenschutzbeauftragte an die Verantwortlichen.

Nicht weniger besorgniserregend sei die Tatsache, dass das Klinikum, teilweise bereits seit vielen Jahren, rund 90 Videokameras mit unterschiedlichen Zielsetzungen einsetze, die weder dem Datenschutzbeauftragten des Klinikums noch einer anderen Stelle jemals angezeigt wurden und deren Zulässigkeit auch zu keinem Zeitpunkt geprüft wurde. „Völlig inakzeptabel ist, dass bis heute keine vollständige Überprüfung der Zulässigkeit des Betriebs der einzelnen Videoanlagen erfolgt ist“, urteilte Klingbeil. In Krankenhäusern könne die Beobachtung bestimmter Bereiche mit Videotechnik zulässig sein, wenn sie beispielsweise zur Wahrnehmung des Hausrechts oder zum Schutz vor Vandalismus oder Diebstahl und Ähnliches erforderlich sei, und dadurch die Persönlichkeitsrechte der Patienten, Besucher und Beschäftigten nicht verletzt würden. Ob die Installation der Kameras im Einzelfall rechens sei oder nicht, bedürfe der Abwägung und Berücksichtigung zahlreicher Kriterien. Vor allem müsse das Krankenhaus kritisch hinterfragen, ob die jeweiligen Überwachungsmaßnahmen erforderlich seien, das festgelegte Ziel mit der Videoüberwachung also erreicht werden könne und es dafür kein weniger in die Persönlichkeitsrechte einschneidendes Mittel gäbe. Daran bestünden nach den Feststellungen vor Ort erhebliche Bedenken. Jörg Klingbeil: „Ich werde alle mir zur Verfügung stehenden aufsichtsrechtlichen Mittel ergreifen, um sicherzustellen, dass nur die den rechtlichen Anforderungen genügenden Anlagen eingesetzt werden.“ Dies könne auch bedeuten, dass einzelne Kameras sofort abzuschalten seien.

Die festgestellten Mängel sind nach Auffassung des Landesdatenschutzbeauftragten wesentlich darauf zurückzuführen gewesen, dass für das große Klinikum mit rund 2 300 Betten und über 6 000 Beschäftigten nur ein betrieblicher Datenschutzbeauftragter bestellt worden sei, der zudem noch weitere Aufgaben erledigen musste und keine Mitarbeiter habe. „Das reicht vorne und hinten nicht, selbst wenn der Betreffende noch so fleißig ist“, kommentierte Jörg Klingbeil die angetroffene Situation. Das Klinikum wolle jetzt Teilaufgaben des Datenschutzes an bestimmte Organisationseinheiten delegieren. Dies könne ein richtiger Schritt sein, um das Datenschutzbewusstsein in der Organisation an mehr Stellen als bisher zu verankern, meinte der Landesbeauftragte abschließend.



Baden-Württemberg

DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ

Anlage 5 zur Pressemitteilung vom 12. Dezember 2011

Sperrfrist: 12. Dezember 2011, 11 Uhr

Landesbeauftragter für den Datenschutz:

Datenschutz in der Arbeitswelt wird immer wichtiger.

(S. 251 ff.)

„Der Datenschutz in der Arbeitswelt hat in meiner Beratungspraxis eine zunehmende Bedeutung. Dies lässt sich bereits nach wenigen Monaten feststellen. Aus diesem Grund ist er auch ein Schwerpunkt meines Berichts.“ Dies erklärte der Landesbeauftragte für den Datenschutz Jörg Klingbeil anlässlich der Vorstellung seines Tätigkeitsberichts am 12. Dezember 2011 in Stuttgart. Erst zum 1. April 2011 hatte er vom Innenministerium die Funktion der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich übernommen. Zahlreiche Bürger und Unternehmen hätten sich im Berichtszeitraum mit Beschwerden und Fragen zum Beschäftigtendatenschutz an ihn, aber auch zuvor an das früher zuständige Innenministerium gewandt.

Ein Großteil der Eingaben von Arbeitnehmern bezieht sich nach den Worten von Jörg Klingbeil auf den Umfang des Fragerechts von Arbeitgebern gegenüber Bewerbern in Bewerbungsverfahren. Nach der Rechtsprechung des Bundesarbeitsgerichts stehe Arbeitgebern ein Fragerecht im Bewerbungsverfahren zu, soweit sie für die Auswahlentscheidung ein berechtigtes und schutzwürdiges Interesse an der Beantwortung ihrer Fragen im Hinblick auf den konkreten Arbeitsplatz und die zu leistende Arbeit haben. Dagegen seien Fragen, die lediglich die Privatsphäre eines Bewerbers betreffen, unzulässig. Deshalb seien Fragen nach dem Familienstand und den Familienverhältnissen eines Bewerbers im Bewerbungsverfahren grundsätzlich ebenso unzulässig wie Fragen nach privaten, nicht arbeitsplatzbezogenen Lebensgewohnheiten, wie z.B. dem Rauchen. Insoweit bestehe regelmäßig kein legitimes Informationsinteresse des Arbeitgebers. Gleiches gelte für allgemeine Fragen nach dem Gesundheitszustand bzw. nach Beschwerden oder Krankheiten sowie die Frage nach der Schwerbehinderteneigenschaft eines Bewerbers. Auch solche Fragen seien in tätig-

keitsneutraler Form, d.h. ohne Bezug zur vorgesehenen Beschäftigung und den damit verbundenen besonderen Anforderungen, in Bewerbungsverfahren unzulässig. Ergänzend hierzu der Landesdatenschutzbeauftragte: „Vielfach beschwerten sich auch Bewerber bei uns, die in einem Auswahlverfahren nicht zum Zuge gekommen waren und danach feststellen mussten, dass der Arbeitgeber die im Zuge des Bewerbungsverfahrens erhobenen Bewerberdaten nicht gelöscht hatte und über die noch gespeicherten Daten auch keine Auskunft gab.“ In solchen Fällen komme die Aufsichtsbehörde nicht umhin, die Arbeitgeber auf ihre Pflichten hinzuweisen.

Jörg Klingbeil weist auch auf einen weiteren Zankapfel zwischen Arbeitgebern und Arbeitnehmern hin: „Es herrscht immer wieder Uneinigkeit darüber, ob und unter welchen Voraussetzungen der Arbeitgeber zur Prüfung der Zuverlässigkeit seiner in sicherheitsrelevanten Bereichen eingesetzten Mitarbeiter von diesen die Vorlage eines Bundeszentralregisterauszugs oder einer Bonitätsauskunft der Schufa verlangen kann. Hier ist im Zweifelsfall ein strenger Maßstab anzulegen. Die Einholung von Auskünften hat sich auf das unbedingt erforderliche Maß zu beschränken.“ Mehrfach beschäftigt habe sich seine Dienststelle auch mit der Zulässigkeit der Erhebung von Gesundheitsdaten in Rahmen von sog. Krankenrückkehrgesprächen, mit der Erhebung von Beschäftigtendaten mittels Ortungstechnik (GPS) oder aus sozialen Netzwerken wie Facebook und nicht zuletzt mit der Videobeobachtung von Arbeitnehmern, insbesondere in Bäckereien und Gaststätten.

Wenn sich Unternehmen mit der Bitte um Beratung an die Aufsichtsbehörde wandten, ging es zumeist um den Transfer von Beschäftigtendaten zwischen Unternehmen innerhalb eines Konzernverbunds, die E-Mail-Kontrolle und den Zugriff auf dienstliche E-Mails von Beschäftigten sowie die Datenerhebung durch konzernweite Compliance-Beauftragte. Auch die Zulässigkeit eines Abgleichs von Beschäftigtendaten mit den sogenannten Antiterrorlisten der EU und der Vereinten Nationen beschäftigte viele Unternehmen.

Hierzu Jörg Klingbeil: „Es ist kein Zufall, dass es sich bei diesen Fragestellungen allesamt um Themen handelt, zu denen mangels detaillierter gesetzlicher Regelungen bislang vielfach Rechtsunsicherheit besteht. Es ist zu hoffen, dass viele der offenen Fragen im Zuge der überfälligen Neuregelung des Beschäftigtendatenschutzrechts beantwortet werden.“



Baden-Württemberg

DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ

Anlage 6 zur Pressemitteilung vom 12. Dezember 2011

Sperrfrist: 12. Dezember 2011, 11 Uhr

**Soziale Netzwerke müssen das deutsche Datenschutzrecht beachten.
Landesbeauftragter mahnt Behörden zur Zurückhaltung bei der Einbindung des
sog. Gefällt-mir-Buttons von Facebook auf ihren Internetseiten.**

(S. 67 ff.)

Der Landesbeauftragte für den Datenschutz, Jörg Klingbeil, hat anlässlich der Vorstellung seines 30. Tätigkeitsberichts am 12. Dezember 2011 in Stuttgart die sozialen Netzwerke aufgefordert, sich mit ihren Angeboten an das deutsche und europäische Datenschutzrecht zu halten. „Soweit eine Datenerhebung auf den Rechnern der Nutzer in Deutschland stattfindet, ist das deutsche Datenschutzrecht anzuwenden. Das trifft insbesondere auf den Marktführer Facebook zu“, erläuterte Jörg Klingbeil. „Wir gehen davon aus, dass die Daten der deutschen Facebook-Nutzer nicht bei der europäischen Niederlassung in Irland, sondern in den USA verarbeitet werden; daher muss auch Facebook den höheren Datenschutzstandard in Deutschland einhalten, ebenso wie seine deutschen Mitbewerber. Dazu gehören größtmögliche Transparenz und restriktive Voreinstellungen – insbesondere zum Schutz von Minderjährigen –, ebenso die Möglichkeit, dass Betroffene ihre Ansprüche auf Auskunft, Berichtigung und Löschung von Daten einfach geltend machen können. Der Zugriff von Suchmaschinen darf nur erfolgen, falls der Nutzer ausdrücklich eingewilligt hat. Außerdem dürfen ohne Einwilligung der Betroffenen keine personenbezogenen Nutzungsprofile gebildet werden.“

Der Landesdatenschutzbeauftragte wies darauf hin, dass das direkte Einbinden von sog. Social Plug-ins, beispielsweise von Facebook, Google+ und Twitter, in Webseiten deutscher Anbieter, eine Datenübertragung an den jeweiligen Anbieter des Social Plug-ins zur Folge habe; dies sei ohne hinreichende Information der Nutzer und ohne die Möglichkeit, dies zu unterbinden, nach dem Telemediengesetz nicht zulässig. Hierzu Jörg Klingbeil: „Die deutschen Webseitenbetreiber tragen eine eigene Verantwortung für die Daten der Nutzer ihres Angebots. Zumindest bei den Social Plug-ins

müssen sie daher Einwilligungserklärungen für die Verarbeitung der Nutzerdaten durch Facebook und Co. einholen. Damit solche Einwilligungserklärungen wirksam sind, sind verlässliche Informationen darüber erforderlich, wofür die Betreiber der sozialen Netzwerke die Daten eigentlich brauchen. Daran fehlt es bis heute.“

Der Landesdatenschutzbeauftragte mahnte insbesondere die öffentlichen Stellen in Baden-Württemberg, dass sie nur solche sozialen Netzwerke in ihre Internet-Auftritte einbinden bzw. dass sie selbst nur solche Netzwerke zur Kommunikation und Außen-darstellung nutzen, die die geltenden Standards nach europäischem und deutschem Datenschutzrecht einhalten: „Die Behörden haben insoweit eine Vorbildfunktion. Es kann nicht sein, dass Bürger, die sich auf den Internetseiten der öffentlichen Stellen unseres Landes informieren wollen, dafür mit ihren Daten bezahlen, die dann zum Rohstoff für eine möglichst individuelle Werbung werden.“ Besonders befremdlich sei in dieser Hinsicht, dass selbst Initiativen, die von der Landesregierung zur Vermittlung von Medienkompetenz für Kinder und Jugendliche gegründet worden seien (zum Beispiel die Initiative Kindermedienland Baden-Württemberg, vgl. www.kindermedienland-bw.de), eine eigene Fanseite auf Facebook unterhielten. Hier wäre etwas mehr kritische Distanz angebracht, um Facebook und Co. zu einem Einschwenken auf die deutschen Datenschutzstandards zu bewegen, meinte Jörg Klingbeil abschließend.