

711.330.1

Sperrfrist: 11 Uhr
27. März 2013

Jahresbericht 2012

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit, Dr. Alexander Dix, stellt heute seinen Tätigkeitsbericht für das Jahr 2012 vor.

Neben den Schwerpunktthemen

- Funkzellenabfragen – von der Ausnahme zur Regel?
- Zehn Vorschläge zur Verbesserung der EU-Datenschutz-Grundverordnung
- BYOD – „Bring your own device“: Arbeiten mit privaten Endgeräten
- Wann dürfen Apothekenrechenzentren Verordnungsdaten weitergeben?
- Wenn die Aufsichtsbehörde klingelt – vermeidbare Fehler von Unternehmen bei Prüfungen

enthält der Bericht 98 Beiträge zur Gesetzgebung und Rechtsprechung, zu Bürgerbeschwerden und Überprüfungen vom Amts wegen in der Berliner Verwaltung und bei Berliner Unternehmen.

Funkzellenabfragen – von der Ausnahme zur Regel? Die Strafverfolgungsbehörden haben das Ermittlungsinstrument wegen unklarer Gesetzesvorgaben quasi alltäglich genutzt, obwohl es eigentlich restriktiv eingesetzt werden muss. Die Staatsanwaltschaft unterliegt hierbei unserer Kontrolle. Ihre gegenteilige Ansicht ist rechtsirrig (**S. 23**).

Wir machen **zehn Vorschläge zur Verbesserung der EU-Datenschutz-Grundverordnung (S. 28)**, mit der das Datenschutzrecht in Europa harmonisiert werden soll. Die Vorschläge betreffen die Rechte der Datenschutzbehörden, der betrieblichen und behördlichen Datenschutzbeauftragten, aber auch die Einwilligung der Betroffenen sowie Auskunfteien und das Scoring.

BYOD – „Bring your own device“ (S. 32): Das **Arbeiten mit privaten Endgeräten** wie Smartphones, Notebooks oder Tablet-PCs am Arbeitsplatz wird immer beliebter. Neben Vorteilen birgt BYOD aber auch Risiken, die durch eine Kombination von technischen und rechtlichen Maßnahmen beherrscht werden müssen.

Wann dürfen Apothekenrechenzentren Verordnungsdaten weitergeben? Angaben zu verkauften Arzneimitteln und zu Rezepten auszuwerten, ist für die Pharmaindustrie sehr interessant. Apothekenrechenzentren dürfen personenbezogene Angaben aber nur zur Abrechnung mit Krankenkassen verarbeiten; für andere Zwecke müssen die Daten anonymisiert werden, damit kein Bezug zum Patienten oder zum Arzt herstellbar ist (**S. 38**).

Wenn die Aufsichtsbehörde klingelt – vermeidbare Fehler von Unternehmen bei Prüfungen (S. 42) sind auch 30 Jahre nach Inkrafttreten des Bundesdatenschutzgesetzes noch häufig. Typische Mängel wurden beobachtet beim Verfahrensverzeichnis, den Verträgen zur Auftragsdatenverarbeitung, bei Lösch- und Sperrkonzepten, aber auch bezogen auf die Auskunftsrechte von Betroffenen sowie die Fachkunde und die Unabhängigkeit der betrieblichen Datenschutzbeauftragten.

Weitere Themen des Jahresberichtes:

Der Einsatz eines **elektronischen Klassenbuches (eKlassenbuch)** wird als IT-Modellprojekt an einigen Schulen getestet. Es ermöglicht auch, Erziehungsberechtigte von unentschuldig fehlenden Schülern zeitnah per SMS zu informieren. Die „**Schulschwänzer-SMS**“ darf aber nur an Eltern versandt werden, die dem zugestimmt haben (**S. 20**).

Die **Antiterrordatei** haben wir erneut **auf den Prüfstand** gestellt: Weder Polizei noch Verfassungsschutz haben das ATD-Gesetz fehlerfrei umgesetzt. Unbeteiligte Personen zu speichern, ist verfassungsrechtlich bedenklich – weshalb sich auch das Bundesverfassungsgericht damit befasst (**S. 48**). Ähnliche Bedenken weckt die **Rechtsextremismus-Datei**. Inwieweit sie neben den vorhandenen Verbunddateien der Sicherheitsbehörden dazu beitragen kann, Fahndungsspannen wie beim NSU zu vermeiden, ist fraglich. Jedenfalls ist sie als **ideenlose Imitation der Antiterrordatei** anzusehen (**S. 49**).

Wiedereinführung der taktischen Hinweise? Die stigmatisierenden Hinweise „Geisteskrank“ und „Ansteckungsgefahr“ haben im polizeilichen Informationssystem nichts zu suchen. Das hat das Abgeordnetenhaus bereits 1988 beschlossen. Warum laut Senatsverwaltung für Inneres und Sport jetzt aus Gründen der Eigensicherung der Polizei etwas anderes gelten soll, ist nicht erkennbar (**S. 55**).

Das neue **Bundesmeldesgesetz** darf nicht den Adresshandel höher bewerten als das Recht des Einzelnen, selbst über die Weitergabe seiner Daten aus dem Melderegister zu bestimmen (**S. 57**). Das jetzt verabschiedete Gesetz trägt dem Rechnung.

Beim Kauf von **Fahrkarten und Parktickets übers Handy** gibt es viele Angebote – nicht alle sind datenschutzfreundlich. Nutzer sollten dasjenige Angebot wählen, das kein umfassendes Bewegungsprofil erstellt (**S. 65**).

Wenn das Finanzamt zur Überprüfung von Fahrschulen bei der DEKRA Prüflisten mit Namen und Anschriften von Prüflingen verlangt, ist das unzulässig. Deren Daten dürfen erst dann erhoben werden, wenn sie für eine konkrete Betriebsprüfung erforderlich sind (**Steuerfahndung in der Fahrschule, S. 75**).

Es verbessert nicht den Kinderschutz, wenn Wohnungsbaugesellschaften verpflichtet werden, Informationen über Familien zu sammeln und Kindeswohlgefährdungen dem Jugendamt zu melden. Stattdessen sollte fachkundiger Rat bei der Hotline Kinderschutz oder dem Krisennotdienst des Jugendamtes eingeholt werden – und zwar ohne Benennung der Familie (**Bezirksamt lädt Vermieter zur Schnüffelei ein, S. 80**).

Die **neue Hygieneverordnung** ist ein wichtiger Durchbruch für den Patientenschutz. Unsere Hinweise zum Schutz der Patientendaten wurden überwiegend berücksichtigt. Noch mehr Transparenz in den medizinischen Einrichtungen würde erzielt, wenn sie verpflichtet wären, die Hygienedaten zu veröffentlichen (**S. 87**). Dafür hat sich auch **die Konferenz der Informationsfreiheitsbeauftragten in Deutschland** ausgesprochen; sie hat zudem bundesweit einheitliche Hygienestandards gefordert (**S. 187**).

Tablet-Computer und Smartphones in der medizinischen Behandlung einzusetzen, birgt mangels Sicherheitsbewusstseins der Hersteller und Nutzer große Risiken. Die Einführung in den Behandlungsalltag eines Krankenhauses muss sorgfältig unter Berücksichtigung von Expertisen zu Informationssicherheit und Datenschutz geplant werden (**Tablet-Computer in der medizinischen Behandlung durch die Charité, S. 95**).

Die im **Berliner Mietspiegel** veröffentlichten Listen mit Änderungswünschen zu bisherigen Wohnlagen und anschließenden Prüfungen konnten Rückschlüsse auf die jeweiligen Antragsteller zulassen. Deshalb war die Veröffentlichung ohne deren Einwilligung unzulässig (**S. 104**).

Können Partner sich gegenseitig für Elterninterviews bevollmächtigen, damit der eine auch Informationen über den anderen preisgeben darf? Dies musste für eine Studie geklärt werden, die die Schul- und Entwicklungsforschung in Bezug auf Schüler und ihr Lebensumfeld betraf (**S. 109**).

Veröffentlichungen von Abiturientendaten in der Tagespresse setzen zwingend voraus, dass die Schulen zuvor die schriftliche Einwilligung der Betroffenen eingeholt haben – ansonsten handeln die Schulen rechtswidrig (**S. 116**).

Informationen über **das Abiturzeugnis des Regierenden Bürgermeisters** sind nur deshalb an die Öffentlichkeit gelangt, weil ein Unbefugter einer Journalistin Einsicht in die Zeugnisse ehemaliger Schüler gewährt hatte. Die vielfältigen Datenschutzverstöße der Schule wurden bei der Senatsbildungsverwaltung beanstandet (**S. 118**).

Unsere Umfrage ergab einen insgesamt zurückhaltenden Einsatz von **Videoüberwachung an Schulen**, was zu begrüßen ist. Wenn wie an wenigen Schulen Videokameras im Haupteingangsbereich und an Fahrradständern angebracht werden, ist das zulässig (**S. 124**).

Ist das ec-cash-Verfahren sicher? Nein, denn es können manuell Transaktionen ausgelöst werden. Die Deutsche Kreditwirtschaft muss diese erhebliche Sicherheitslücke durch technische Maßnahmen schließen; vertragliche Absicherungen reichen nicht aus (**S. 129**).

Vorsicht bei Online-Bonitätsprüfungen! Um das Ausfallrisiko beim Kauf auf Rechnung zu minimieren, führen Online-Shops Bonitätsprüfungen durch – oft heimlich. Abhängig von der Gestaltung des Bestellprozesses ist vorab die Einwilligung der Betroffenen einzuholen (**S. 131**).

Erstmals gibt es einen mit allen Aufsichtsbehörden abgestimmten Verhaltenskodex für eine gesamte Branche, nämlich die Versicherungswirtschaft. Dem Gesamtverband der Deutschen Versicherungswirtschaft haben wir die Vereinbarkeit mit dem Datenschutzrecht attestiert (**Bundesweite Premiere: Anerkennung von Verhaltensregeln nach dem BDSG, S. 147**).

Die **Informationspflicht bei Datenlecks in Wirtschaft und Verwaltung** muss konsequenter erfüllt werden. Häufig werden zwar die Aufsichtsbehörden benachrichtigt, aber nicht die Betroffenen (**S. 149**).

Anschluss- und Benutzungszwang bei Facebook? Diensteanbieter sind rechtlich verpflichtet, den Nutzenden eine anonyme oder pseudonyme Nutzung zu ermöglichen. Es ist unzulässig, wenn Diensteanbieter die Registrierung ausschließlich über ein soziales Netzwerk wie Facebook anbieten, das auf einer Registrierung unter Klarnamen besteht (**S. 166**).

Intelligente Werbeflächen sind die neueste Innovation der Werbebranche. Per Videotechnik werden Live-Bilder von dem zu bewerbenden Produkt und Passanten bzw. vorbeifahrenden Autos erzeugt. Unter welchen Voraussetzungen ist das zulässig? (**S. 180**)

Die **Organisation des Datenschutzes in den Bezirken** ist zum Teil mangelhaft. Das hat unsere Umfrage bei den behördlichen Datenschutzbeauftragten ergeben. Wenn sie – wie in Pankow und Lichtenberg – zugleich die Aufgaben des Antikorruptionsbeauftragten wahrnehmen, ist das wegen des Interessenkonflikts rechtswidrig (**S. 184**).

Die **Informationsfreiheit in Berlin** muss weiterentwickelt werden. Dieses Ziel verfolgt auch die Fraktion Bündnis 90/Die Grünen mit ihrem **Entwurf eines Berliner Transparenz- und Informationsfreiheitsgesetzes**, das einen Paradigmenwechsel vollziehen soll: Informationszugang für die Bürger nicht erst auf Antrag, sondern pro-aktiv von Amts wegen. Auch die von uns geforderte **verfassungsrechtliche Verankerung des Anspruchs auf Informationszugang** würde in der Bundeshauptstadt ein bedeutsames Signal für noch mehr Transparenz setzen (**S. 188**).

Viel Ärger um Senatsbeschlüsse gab es mit der Senatskanzlei, die die Herausgabe an einen Bürger unter Hinweis auf die Geschäftsordnung des Senats hartnäckig verweigerte. Diese Verwaltungsvorschrift ist allerdings rechtswidrig, weil sie dem Berliner Informationsfreiheitsgesetz zuwiderläuft, und muss deshalb geändert werden (**S. 191**).

Wenn öffentliche Stellen keine allgemein zugänglichen Aktenpläne haben, verstößt das gegen das Berliner Informationsfreiheitsgesetz. Sie sind die Grundvoraussetzung für detaillierte Informationsanfragen der Bürger bei öffentlichen Stellen (**Aktenpläne im Bezirksamt Treptow-Köpenick – und deren Zweck, S. 201**).

Was die Menschen sonst noch von unserer Tätigkeit haben, wird im vorletzten Kapitel knapp erläutert. So haben wir bewirkt, dass ein Krankenhaus künftig Patientendaten nur noch mit schriftlicher Zustimmung des Patienten und über einen besonders geschützten Faxbereich verschickt, nachdem es irrtümlich Patientendaten an einen unbeteiligten Bürger gefaxt hatte (**S. 204**).

Der Jahresbericht ist im Internet unter der Adresse www.datenschutz-berlin.de abrufbar.