

## Literaturüberblick

### **Unabhängige Datenschutzaufsicht**

Wer kontrolliert den Kontrolleur? - Im Vorgriff auf das mittlerweile ergangene Urteil des Europäischen Gerichtshofs (EuGH) in der Rechtssache C-518/07 erörtern Thomas Petri und Marie-Theres Tinnfeld in ihrem Aufsatz „Völlige Unabhängigkeit der Datenschutzaufsicht“ in der Zeitschrift *MultiMedia und Recht* (MMR 3/10, Seite 157), wie sich eine unabhängige Datenschutzaufsicht im nicht-öffentlichen Bereich ohne demokratisches Legitimationsdefizit verwirklichen lässt. Die Autoren gelangen zu dem Ergebnis, dass die Datenschutzaufsicht eine Kontrollinstanz „eigener Art“ sei, die sich nicht einseitig der staatlichen Verwaltung zuordnen lasse. Sie geben zudem hilfreiche Anregungen, wie die drei Vorgaben des EuGH für die Datenschutzaufsicht im nicht-öffentlichen Bereich - Freiheit von staatlicher Aufsicht bei zulässigem parlamentarischen Einfluss und steter Kontrolle durch die zuständigen Gerichte - jetzt umgesetzt werden können.

■ SHA

### **ELENA**

Die Datenübermittlung und -speicherung auf Grund des Gesetzes über den Elektronischen Entgeltnachweis (ELENA) stößt auf erhebliche Kritik und hat auch zu einer Verfassungsklage geführt. In der Zeitschrift *Computer und Arbeit* (CuA 2/10, Seite 26) schildert Achim Thanheiser, was mit ELENA erreicht werden soll, welche Beschäftigten-daten übermittelt werden sollen und ob die Belegschaftsvertretung bei ELENA ein Mitbestimmungsrecht hat. Sein Fazit: „Die

elektronische Übermittlung von Daten der Beschäftigten an eine zentrale Stelle ist ein mitbestimmungspflichtige Maßnahme. Da dem Betriebs- und Personalrat die Kontrolle über die Einhaltung von Datenschutzregeln zugunsten der Beschäftigten obliegt, ist er zu beteiligen.“ In der gleichen CuA-Ausgabe (Seite 28) beschreibt Jochen Konrad-Klein das technische Verfahren von ELENA. ■ HK

### **Grundfragen der Datenschutz-Compliance**

„Nach den echten und vermeintlichen Datensandalen bei Deutscher Bahn, Lidl, Aldi & Co. hat das Thema Compliance die Schlagzeilen erobert. Inzwischen ist weitgehend unbestritten, dass der Vorstand einer unabhängigen Aktiengesellschaft einer einzel-fallabhängigen Pflicht zur Compliance unterliegt. In den Fokus rückt nunmehr die Frage, ob auch den Vorstand einer Konzernmutter eine Compliance-Pflicht in Bezug auf verbundene Unternehmen trifft – hier scheiden sich die Geister. Vernachlässigt wird weiterhin, dass der Datenschutz nicht Gegner, sondern Gegenstand der Compliance ist.“ Mit diesen einleitenden Sätzen ist der Beitrag von Dr. Gerrit Forst in der Zeitschrift *Datenschutz und Datensicherheit* (DuD 3/10, Seite 160) versehen. ■ HK

### **WLAN-Sicherheit**

Eine aktuelle Studie der TU Ilmenau untersucht die Sicherheit von Wireless Local-Area-Networks in deutschen Behörden und Unternehmen. Begleitend dazu wurde ein Katalog von WLAN-Sicherheitsmaßnahmen entwickelt. In der Zeitschrift für Kommunikation- und EDV-Sicherheit (kes 1/10,

Seite 66) stellt Dr. Daniel Fischer die Studie vor und erläutert den WLAN-Sicherheitsmaßnahmen-Katalog. ■ HK

### **Privatdetektiv**

„Einsatz eines Privatdetektivs im Arbeitsrecht“ – der Beitrag von Götz A. Maier und Stefan Garding in der Zeitschrift *Der Betrieb* (DB 10/10, Seite 559) fasst die Entscheidungen der Arbeitsgerichte zum Einsatz von Privatdetektiven zusammen. Maier und Garding gehen auch auf die Auswirkungen des neuen § 32 BDSG ein und schließen sich der Auffassung an, dass durch ihn § 28 nicht vollständig verdrängt wird. ■ SF

### **Rechtliche Aspekte der IT-Sicherheit**

Dr. Michael Schmidl beschreibt in der *Neuen Juristischen Wochenschrift* (NJW 8/10, Seite 476) mögliche Ausgangspunkte für die Analyse der IT-Sicherheit im Unternehmen, die vielfältigen verschiedenen Elemente des Rechts der IT-Sicherheit und die rechtlichen Grenzen, die bei der Umsetzung von Maßnahmen der IT-Sicherheit zu berücksichtigen sind. ■ HK

### **Zulässigkeit von spickmich.de**

Personenbezogene Bewertungsportale wie meinprof.de und spickmich.de für Lehrer werfen rechtliche Fragen im Hinblick auf Persönlichkeits- und Datenschutz im Spannungsfeld mit den Kommunikationsfreiheiten auf. Mit dieser Kollision von Rechtspositionen befassen sich Prof. Dr. Georgios Gounalakis und Catherina Klein, Universität Marburg, in der *Neuen Juristischen Wochenschrift* (NJW 9/10, Seite 566) auf der Grundlage des Ur-

teils des Bundesgerichtshofs zur der Lehrer-Bewertungsplattform „spickmich.de“ (DSB 7+8/09, Seite 30). Der Beitrag zeigt die Zulässigkeitsvoraussetzungen und rechtlichen Grenzen personenbezogener Bewertungsforen anhand der aktuellen Rechtsprechung auf. ■ HK

### Meldung von Datenschutzpannen

„Im Rahmen der im letzten Jahr erfolgten Novellierung des Bundesdatenschutzgesetzes (BDSG) wurde eine Informationspflicht bei sogenannten Datenschutzpannen eingefügt. Diese neue Vorschrift, § 42a BDSG, betrifft auch das Arbeitsverhältnis. Sie soll es den Betroffenen und den Datenschutzaufsichtsbehörden erleichtern, bei Datenverlusten – das heißt, wenn die genannten sensiblen Daten unrechtmäßig in die Hände Dritter gelangt sind – Folgeschäden zu vermeiden.“ So Prof. Dr. Gola zu Beginn seines Aufsatzes „Information über Datenschutzpannen auch gegenüber Arbeitnehmern“ in Computer und Arbeit (CuA 2/10, Seite 33). ■ HK

### Bewerberdaten „googeln“?

„Bewerberdaten – was darf `er-googelt´ werden?“ Dieser Frage geht Prof. Peter Gola in seinem Aufsatz in der Zeitschrift Computer und Arbeit (CuA 3/10, Seite 31) nach. Der Aufsatz ist mit folgender Einleitung versehen: „So manche Information über Bewerber, nach der direkt zu fragen dem Arbeitgeber gemäß der datenschutzrechtlichen Grenzen seines `Fragerechts´ nicht gestattet wäre, stellt ihm das Internet ohne Probleme zur Verfügung. Schließlich nutzen auch Personaler mittlerweile ausgiebig Suchmaschinen und das Web 2.0. Politische oder religiöse Aktivi-

täten sind dort ebenso veröffentlicht wie private Vorlieben oder sexuelle Wünsche. Zumeist sind auch Fotos hinterlegt. Ins Netz gelangen diese Informationen einmal durch den Betroffenen selbst, zum anderen handelt es sich aber auch um Drittquellen. Abgesehen von der Zulässigkeit derartiger Recherchen: Wehren kann man sich dagegen in der Regel nicht.“ ■ HK

### Videoüberwachung

Bruno Schierbaum stellt in seinem Beitrag „Videoüberwachung – der aktuelle Stand“ in Computer und Arbeit (CuA 2/10, Seite 5) die wichtigsten Gerichtsentscheidungen zur Videoüberwachung am Arbeitsplatz vor und erörtert die Auswirkungen der aktuellen Änderungen im BDSG auf die Videoüberwachung. Karl-Heinz Böker beschreibt (Seite 13), was in einer Betriebs-/Dienstvereinbarung zum Einsatz einer Videoüberwachungsanlage konkret geregelt werden sollte und darin die Persönlichkeitsrechte der Beschäftigten effektiv geschützt und gefördert werden können. ■ HK

### Cloud Computing und Strafverfolgung

„Cloud Computing als neue Herausforderung für Strafverfolgungsbehörden und Rechtsanwaltschaft“ ist der Beitrag von Nils Obenhausen in der Neuen Juristischen Wochenschrift überschrieben (NJW 10/10, Seite 651). Mit der Struktur des „Cloud Computing“ lagern alle Programme und vor allem die Daten auf den Servern der Anbieter. Damit können auch Daten, die der Begehung von Straftaten dienen, an verschiedenen Orten abgespeichert werden, Obenhausen geht der Frage nach, wie die Strafverfolgungsbehörden von solchen Datenbeständen Kenntnis erlan-

gen können und welche Hindernisse dabei bestehen. ■ HK

### Weitergabe von IP-Adressen

Joerg Heidrich und Dr. Christoph Wegener gehen in der Zeitschrift Datenschutz und Datensicherheit (DuD 3/10, Seite 172) der Frage nach, welche konkreten technischen und rechtlichen Konsequenzen sich daraus ergeben, dass es sich bei IP-Adressen um personenbezogene Daten handelt. ■ HK

### Softwaresicherheit

Das Märzheft der Zeitschrift Datenschutz und Datensicherheit lässt eine Reihe international anerkannter Experten auf dem Gebiet der Verbesserung der Softwarequalität zu Wort kommen. In dem Aufsatz „Security Development Lifecycle“ (Seite 135) stellt Steve Lipner dar, wie die Prinzipien der sichereren Softwareentwicklung bei Anwendungen im Cloud Computing einzusetzen sind.

Kai Jendrian beschreibt die Standardisierung der Sicherheitsüberprüfung von Web Anwendungen nach dem Modell der OWASP (Seite 138). In dem Beitrag „Platform for Application Risk Intelligence“ (Seite 143) stellt Maty Siman eine Plattform zur Code Analyse hinsichtlich Sicherheitslücken von Anwendungen vor. Darauf aufbauend liefert der Beitrag „Prioritizing Static Analysis Results“ (Seite 156) von Brian Chess und Jacob West einen Ansatz, die Ergebnisse solcher Testautomaten nach Risiken für den Anwender zu priorisieren. Der Artikel von Chris Wysopal, Chris Eng und Tyler Shields „Static Detection of Application Backdoors“ (Seite 149) geht auf die Prüfung von vorsätzlich in den Code eingefügter „Hintertüren“ ein. ■ HK