

**Die 8. Jahreskonferenz des FFD Forum für Datenschutz fand am 20. und 21. April 2010 in Mörfelden-Walldorf bei Frankfurt/Main statt. Unter dem Motto „Das neue Datenschutzrecht- Auswirkungen auf den betrieblichen Datenschutz-Mitarbeiterüberwachung aktuell“ referierten Vertreter aus Wirtschaft, Wissenschaft und Politik zum aktuellen betrieblichen Datenschutz.**

**Von MARKUS SELENT, Berlin.**

Die ehemalige Bundesjustizministerin Prof. Dr. Hertha Däubler-Gmelin eröffnete die Veranstaltung, war aber letztlich durch die Sperrung des europäischen Luftraums am persönlichen Vortrag gehindert. Sie kritisierte, wenn sich wirtschaftliche Interessen gegen den Datenschutz stemmten, weil Daten-

schutz Bürokratie und Kosten bedeute. Beide seien unnötig, gar schädlich. Daher würde über Lobbyarbeit versucht, Anforderungen abzumildern oder zu verhindern. Besonders deutlich sei dies an der „berüchtigten Kompromissformulierung“ des neuen § 32 BDSG. Die Auseinandersetzung um den Beschäftigungsdatenschutz sei daher keineswegs beendet. Herbe Kritik übte Däubler-Gmelin auch an ELENA (Elektronischer Entgeltnachweis); es zeige, wie mit Arbeitnehmerdaten möglichst nicht umgegangen werden sollte.

### **Vorratsdatenspeicherung**

Hans-Hermann Schild, Richter am Verwaltungsgericht Wiesbaden, stellte klar, dass unter gewissen Voraussetzungen, die das Bundesverfassungsgericht vorgegeben habe (anspruchsvolle normenklare

Regelungen zur Datensicherheit, Datenverwendung, der Transparenz und des Rechtsschutzes), gesetzliche Regelungen zur Vorratsspeicherung möglich seien. Ein Blick in die Zukunft zeige, dass sowohl auf europäischer als auch auf nationaler Ebene eine entsprechende politische Diskussion in Gang gesetzt wurde. Auch der Europäische Gerichtshof werde sich in den verbundenen Rechtssachen C-92/09 und C-93/09 zur Richtlinie 2006/24/EG äußern.

## **BDSG-Novellierung**

Dr. Philipp Kramer referierte mit besonderem Fokus auf die Auftragsdatenverarbeitung über die aktuellen Änderungen im Bundesdatenschutzgesetz (BDSG). Kramer zufolge bedeute – jedenfalls theoretisch in einem bisher perfekt arbeitenden Unternehmen - der neue § 11 BDSG weder erhöhte Anforderungen noch liege ein erhöhtes Arbeitsaufkommen für den betrieblichen Datenschutzbeauftragten vor. Bei der Umsetzung liege das Hauptproblem in der Kontrolle des Dienstleisters (Vor-Ort-Kontrolle oder „Papierkontrolle“). Gegen eine Vor-Ort-Kontrolle spräche der Aufwand, je nach Unternehmenssitz seien erhebliche Wege in Kauf zu nehmen. Darüber hinaus sei der Umfang der Kontrolle vor Ort kaum zu überblicken und der Zugang bei den Dienstleistern schwierig durchzusetzen. Bei einer Papierkontrolle reiche es nicht, nur die entsprechenden Erklärungen entgegenzunehmen. Es seien auch Unterlagen und Belege anzufordern, um die entsprechenden Erklärungen zu überprüfen. Soweit bereits Kontrollen durch die Aufsichtsbehörden durchgeführt worden seien, können deren Prüfungsbelege hilfreich sein. Als vorteilhaft stellte sich bisher heraus, wenn Fragenkataloge durch die Dienstleister ausgefüllt wurden und die Ergebnisse hieraus anhand von Belegen überprüft werden.

Dr. Robert Selk nahm zu den Problemkreisen Auftragsdatenverarbeitung und Cloud Computing Stellung. Die Aufsichtsbehörden würden bei der Anpassung der Auftragsdatenverarbeitungsverträge an die Novellierung meist eine faktische Übergangsfrist gewähren, die aber im ersten Halbjahr 2010 auslaufe. Zu § 11 BDSG merkte Selk an, dass eine Vor-Ort-Prüfung nicht zwingend sei. Eine schriftliche Selbstauskunft des Auftragnehmers reiche aber meist – da nicht neutral genug – nicht aus. Unabhängige Audits seien besser geeignet. Da der Auftraggeber die Verantwortung für den richtigen Maßstab des „Überzeugens“ trage, sei es in der Praxis besser, zuviel als zu wenig zu prüfen. Im Cloud Computing, so Selk, sei eine Auf-

tragsdatenverarbeitung derzeit nicht umsetzbar. Zunächst würden schon Zweifel bestehen, ob der Auftraggeber tatsächlich noch Herr der Daten sei. Dies setze nach derzeitiger Ansicht die genaue Kenntnis des Ortes der Verarbeitung, mithin der Speicherung voraus, was bei großen weltweit operierenden Clouds nahezu unmöglich sei. Darüber hinaus scheide wegen § 3 Abs. 8 Satz 3 BDSG bei globalen Clouds eine Auftragsdatenverarbeitung aus, da diese nicht innerhalb der Europäischen Union stattfinde. Spätestens bei der Erfüllung der Verpflichtungen nach § 11 Abs. 2 Satz 4 BDSG seien die Grenzen des Umsetzbaren erreicht. Die Überprüfung der technischen und organisatorischen Maßnahmen beim Cloud Provider sei faktisch nicht realisierbar.

Dr. Thomas Petri, Bayerischer Landesbeauftragter für den Datenschutz, richtete seinen Blick auf die Stellung der Aufsichtsbehörde nach der BDSG-Novellierung. Nach seiner Auffassung habe die Aufsichtsbehörde aufgrund der Europäischen Datenschutzrichtlinie auch den Auftrag zur demokratischen Rückkopplung, mithin eine Beratungsfunktion gegenüber Parlament, Regierung und Öffentlichkeit. Ihre Tätigkeitsberichte sollten aktuellen Fehlentwicklungen entgegenwirken. Neben der Anordnungs- und Untersagungsbefugnis nach § 38 Abs. 5 BDSG komme der Aufsichtsbehörde eine weitere Bedeutung bei der Aufarbeitung von Datenpannen nach § 42a BDSG zu. So liege die Feststellungsbefugnis der Tatbestandsvoraussetzungen in beiden Fällen bei der Aufsichtsbehörde. Daher sei aufgrund der Bußgeldbewehrung dringend geraten, unmittelbar tätig zu werden. Die Frage, inwieweit ein „Dritter“ im Sinne von § 42a BDSG verpflichtet ist, die Aufsichtsbehörde zu unterrichten, wurde dahingehend erörtert, dass eine teleologische Reduktion des Tatbestandes in Betracht komme. Eine Meldepflicht könne daher nicht ohne weiteres auch auf den Dritten ausgeweitet werden. In einem Ausblick machte Petri deutlich, dass aufgrund der Entscheidung des Europäischen Gerichtshofs zur Unabhängigkeit der Datenschutzaufsicht eine Umstrukturierung erfolgen werde. Wie dies umgesetzt werde, sei nicht konkret vorherzusehen. Eine Ausgliederung bringe aber einige Probleme mit sich.

Ralf Maruhn befasste sich mit Stellung, Haftung und dem Kündigungsschutz des betrieblichen Datenschutzbeauftragten nach der BDSG-Novellierung. Maruhn zufolge kommt eine zivilrechtliche Haftung des betrieblichen Datenschutzbeauftragten nur

selten in Betracht. § 4f BDSG stelle kein Schutzgesetz im Sinne des § 823 Bürgerliches Gesetzbuch (BGB) dar. Aus dem Bestellungsvertrag hafte der Datenschutzbeauftragte nur gegenüber seinem Dienstherrn. Ein direkter Durchgriff Dritter auf den Datenschutzbeauftragten sei nicht möglich. Auch juristische Konstruktionen wie der Vertrag zugunsten Dritter nach § 323 BGB oder der Vertrag mit Schutzwirkung zugunsten Dritter fänden keine Anwendung. Allerdings sei es nicht nur in Anbetracht des Compliance-Urteils des Bundesgerichtshofes (DSB 11/09, Seite 18, DSB 4/10, Seite 13) ratsam, die Kompetenzen und Aufgabenbereiche des betrieblichen Datenschutzbeauftragten detailliert zu beschreiben. So könne in der Bestellung auch eine konkrete Regelung über eine Haftungsbegrenzung oder -freistellung getroffen werden.

## **Beschäftigtendatenschutz**

Hans-Hermann Schild äußerte sich kritisch zum Eckpunktepapier des Bundesinnenministeriums zum Beschäftigtendatenschutz. Die Orientierung an unbestimmten Rechtsbegriffen wie „Erforderlichkeit“ trage nicht zur Rechtssicherheit bei. Darüber hinaus ergebe sich aus dem Eckpunktepapier, dass weder Regelungen zur Stellung des betrieblichen Datenschutzbeauftragten gegenüber dem Betriebsrat noch eine zufriedenstellende Lösung im Umgang mit Internet und E-Mail durch die Beschäftigten getroffen werde.

Prof. Dr. Marie Theres Tinnefeld beleuchtete das Whistleblowing im Spannungsfeld zum Beschäf-

tigtendatenschutz. Unternehmen sei regelmäßig daran gelegen, Informationen über Korruption oder Missstände zu erhalten. Dennoch würden Whistleblower ein erhöhtes Risiko eingehen, berufliche Nachteile oder Mobbing zu erleiden. Tinnefeld führte aus, dass § 32 Abs. 1 Satz 2 BDSG die Verwendung von Beschäftigtendaten durch den Arbeitgeber für die Aufklärung von Straftaten regele. Eine Rechtsgrundlage für die Aufklärung anderer Compliance-Verstöße stelle die Vorschrift nicht dar, hier könne § 32 Abs. 1 Satz 1 BDSG Anwendung finden. Außerhalb der Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses komme dann die Interessenabwägung nach § 28 Abs. 2 Nr. 2a BDSG in Betracht. Die Neuregelung, so Tinnefeld, sei aber nicht geeignet, schwierige Fälle im Bereich des Whistleblowings angemessen zu lösen. Ausweg könne eine Betriebs- oder Dienstvereinbarung als Rechtsnorm im Sinne des § 4 Abs. 1 BDSG sein. Die Betriebspartner seien, wie es sich auch etwa § 75 Abs. 2 Betriebsverfassungsgesetz ergebe, verpflichtet, das allgemeine Persönlichkeitsrecht der Beschäftigten zu schützen und zu fördern. Vereinbarungen auf dieser Ebene würden bis zur Schaffung eines umfangreichen Beschäftigtendatenschutzes auch Möglichkeiten geben, allen Beteiligten die notwendige Rechtssicherheit zu gewähren. ■

Stichworte: FFD, Beschäftigtendatenschutz, Novellierung, Cloud Computing, Auftragsdatenverarbeitung, Whistleblowing