

samkeit nicht aufs Spiel zu setzen. Im Bereich beruflicher Geheimnisse stellte Schmidl klar, dass eine Weitergabe der Daten ohne ausdrückliche Einwilligung kaum möglich sei. Um für Berufseheimnisträger wie Ärzte oder Rechtsanwälte den Straftatbestand des § 203 Strafgesetzbuch bei der Auftragsdatenverarbeitung zu umgehen, schlug Schmidl vor, den Auftragnehmer über einen sogenannten Gehilfenvertrag zu binden, um dadurch weitere Kontrollbefugnisse zu erlangen. Auf diesem Wege wäre es dem Geheimnisträger möglich, Weisungen auch direkt gegenüber Beschäftigten des Auftragnehmers durchzusetzen, um die Kontrolle der Daten zu gewährleisten. Hierzu zähle dann auch das Recht, einzelne Beschäftigte auszutauschen. Ein solch weitgehender Eingriff in die Autonomie des Auftragnehmers wurde bezüglich der praktischen Umsetzbarkeit von den Zuhörern kontrovers diskutiert. Rechtsanwältin Dr. Christiane Bierehoven konstatierte beim Thema Cloud Computing gerade bei der „public cloud“, also dem Serverbetrieb außerhalb einer unternehmensspezifischen Kontrolle, erhebliche datenschutzrechtliche Bedenken. Hinsichtlich einer Auftragsdatenverarbeitung verliere der Auftraggeber schnell die Beherrschbarkeit, da die Daten auf unterschiedlichsten Systemen weltweit verstreut sein können. Die Durchführung einer

Vorabkontrolle sei kaum zu bewerkstelligen. Auch der Ausschluss von Zugriffsmöglichkeiten durch Dritte kann in der jetzigen Form des Cloud Computing kaum gewährleistet werden. Jedenfalls die „public cloud“ sei nach § 11 BDSG nicht zulässig.

ELENA und Personalausweis

Der Vortrag der Referatsleiterin der Deutschen Rentenversicherung Bund Claudia Hesse über ELENA zeigte, wie viel Explosionsstoff in dem Thema steckt. Die Diskussion bewegte sich zwischen dem Hinweis der Ersparnis für die deutsche Wirtschaft von jährlich EUR 85 Mio. und dem Verstoß gegen den Grundsatz der Datensparsamkeit und die Karlsruher Vorgaben zur Vorratsdatenspeicherung. Ministerialrat Andreas Reisen stellte die praktischen Vorzüge des neuen Bundespersonalausweises dar. Die Diskussion zeigte, dass es noch Handlungsbedarf gibt. Eine verpflichtende umfassende Prüfung des Datenschutzes bei den jeweiligen Anbietern und Nutzern der Daten des Bundespersonalausweises finde nicht statt, wodurch die Gefahr des Missbrauchs der Daten durch Dritte nicht ausgeschlossen sei. ■

Stichworte: DuD-Fachkonferenz, Schaar, Casper, Auftragsdatenverarbeitung, ELENA, Personalausweis

Der Datenschutzbeauftragte informiert: Urlaubszeit - die unterschätzte Gefahr

Viele Reisende möchten oder können im Urlaub nicht auf die elektronische Kommunikation verzichten. Die Sorglosigkeit von Touristen gepaart mit der kriminellen Energie von Straftätern führt zu unberechenbaren Risiken in Internetcafés im Hinblick auf einen Datenverlust. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) weist aktuell auf die oftmals mangelnde Aktualität der Schutzprogramme oder die heimliche Installation von Spionageprogrammen in Internetcafés hin. Bitte verzichten Sie bei der Nutzung von allgemein zugänglichen Rechnern im Urlaub auf die Durchführung von Bankgeschäften und den Abschluss von Kaufverträgen. Sie übermitteln vertrauliche Daten, die von Kriminellen – bei unzureichender Sicherung des PC – abgefangen und für ihre Zwecke genutzt werden können. Das BSI rät bei Internetcafés zu folgenden Schutzmaßnahmen: (1) Kontrolle der Aktualität der Schutzsoftware, (2) Manuelle Eingabe der Internetadresse, (3) Löschung des Verlaufverzeichnisses im Browser. Des Weiteren sollten Sie sensible Informationen nur verschlüsselt übertragen, wichtige Angaben ausdrucken, Kon-

tenbewegungen überprüfen und ein Tageslimit für Geldgeschäfte gegenüber Ihrer Bank festlegen.

Öffentliche, ungesicherte WLAN-Hotspots stellen ebenfalls eine Gefahr dar. Daher sollten Sie, soweit möglich, auf die Einwahl mittels WLAN verzichten. Das BSI empfiehlt folgende Maßnahmen für ein gefahrloseres Surfen: (1) Nutzung eines aktuellen Betriebssystems, Virenschutzprogrammes und Firewall, (2) Keine Anmeldung als Administrator, sondern als User mit eingeschränkten Zugriffsrechten, (3) Deaktivierung der Datei- und Verzeichnisfreigabe für das Netzwerk, (4) Verschlüsselung von sensiblen Informationen, (5) Sicherung von wichtigen Daten. ■ NSCH

Wir empfehlen unseren Lesern, diesen Text als Mitarbeiterinformation hausintern zu verwenden.

Internet:
www.bsi.bund.de/cln_156/ContentBSIFB/Aktuelles/Brennpunkt/urlaub.html; www.bsi.bund.de/ContentBSIFB/Aktuelles/Brennpunkt/sicher_unterwegs_mit_handy_laptop.html

Stichworte: Datendiebstahl, Hotel, Urlaub, Internetcafe