

denn, der Betroffene habe dem ausdrücklich zugestimmt, Artikel 6 (1) b und Artikel 7a der Richtlinie 95/46/EG.

Ausblick

Die Stellungnahme enthält keine Aussagen über die technologischen Mittel, die eingesetzt werden sollten, um die Ziele der Stellungnahme zu erreichen. Stattdessen wird die Industrie in der Stellungnahme mehrmals dazu aufgefordert, mit der Artikel 29-Gruppe in einen Dialog zu treten, um technische und sonstige Mittel zur schnellstmöglichen Einhaltung des in der Stellungnahme dargelegten Rechtsrahmens zu unterbreiten. Die EU-Mitgliedstaaten

müssen die novellierte ePrivacy-Richtlinie bis Mai 2011 in ihr nationales Recht umsetzen. Es wird sich zeigen, wie die Mitgliedstaaten Artikel 5 (3) umsetzen und ob diese den Interpretationen der Aufsichtsbehörden folgen werden. ■

* Der Autor ist Rechtsanwalt in der Kanzlei Hunton & Williams, Brüssel.

Internet:
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_de.pdf

Stichworte: Cookies, ePrivacy-Richtlinie, Europa, Artikel 29-Datenschutzgruppe, Werbung, Website-Betreiber, Werbenetzwerk, Browser, Online-Profiling

DSRI-Herbstakademie 2010

Vor allem das Datenschutzrecht stand im Fokus der etwa 200 Teilnehmer der Herbstakademie der Deutschen Stiftung für Recht und Informatik (DSRI), die unter dem Leitthema „Digitale Evolution“ vom 9. bis 11. September in München stattfand. Die Referenten aus der Anwaltschaft beleuchteten den Regierungsentwurf zum Beschäftigtendatenschutz und die novellierungsbedingten Änderungen bei der Auftragsdatenverarbeitung.

Von STEFAN FELIXBERGER, Osterhofen.

Dr. Flemming Moos widmete sich im „Update Datenschutzrecht“ zunächst der bis Mai 2011 anstehenden Umsetzung der Europäischen Datenschutzrichtlinie zur elektronischen Kommunikation (DSB 1/10, Seite 4 und DSB 3/10, Seite 8). Interessant wird dabei die Thematik der Opt-In-Pflicht für Werbe-Cookies. Nach einem Arbeitspapier der Artikel 29-Datenschutzgruppe soll die Browser-Einstellung als Zustimmung dafür nicht ausreichen (siehe vorangegangener Beitrag). Für Crossborder E-Discovery-Fälle empfahl Diana Kunst präventive Maßnahmen (Data Retention Policy). Die Vorlagepflichten erstreckten sich faktisch auf alle konzernverbundenen Gesellschaften. In der Praxis könne man sich an der Stellungnahme der Artikel 29-Gruppe (DSB 4/09, Seite 10), einer Empfehlung der französischen Aufsichtsbehörde CNIL und Ausführungen der Sedona Conference orientieren.

Beschäftigtendatenschutz

Dr. Marc Philipp Weber stellte den Regierungsentwurf zum Beschäftigtendatenschutz kritisch vor.

Er sieht weiterhin ungelöste Abgrenzungsprobleme (Was fällt unter „Zweck eines Beschäftigungsverhältnisses“?). Betriebsvereinbarungen dürften nach dem Regierungsentwurf das gesetzliche Schutzniveau nicht unterschreiten, sondern nur Abläufe gestalten oder Bestimmungen konkretisieren; sie könnten auch keine heimliche Videoüberwachung rechtfertigen. Bei den geplanten Einschränkungen bei der Einwilligung (nur noch zulässig, soweit im neuen Unterabschnitt ausdrücklich vorgesehen) sieht Weber mögliche europarechtliche und verfassungsrechtliche Bedenken. § 32e des Regierungsentwurfes enthalte viele unbestimmte Rechtsbegriffe, so dass es schwierig sei, belastbare Konzepte zu entwickeln. Offen bleibe auch nach dem Regierungsentwurf, ob das Fernmeldegeheimnis bei zugelassener Privatnutzung bei Verdacht einer Straftat durchbrochen werden dürfe; hier sei eine Überarbeitung nötig. Florian Albrecht widmete sich Verhaltensanalysen bei Bewerbern (siehe DSB 3/10, Seite 11). Bei der Prüfung der „Erforderlichkeit“ (§ 32 Bundesdatenschutzgesetz - BDSG) sieht er drei „Auslegungs-Lager“:

- Subjektive Bestimmung aus Sicht des Arbeitgebers
- Unverzichtbarkeit zu betrieblichen Zwecken
- Anwendung des Grundsatzes der Verhältnismäßigkeit mit konkreter Interessenabwägung im Einzelfall.

Beim Thema „Datenabgleich zur Korruptionsbekämpfung“ sind David Seiler zufolge mit völlig anonymer Kontrolle die Anforderungen an die Risikovermeidung nicht zu erreichen. Es müssten

– gerade auch bei Banken – personenspezifische Risiken ermittelt werden.

Auftragsdatenverarbeitung

Dr. Anna Gosche berichtete über Praxiserfahrungen zum novellierten § 11 BDSG. Altverträge scheitern zu 99 Prozent an den neuen Anforderungen. Bei § 11 Nr. 2 BDSG reichen pauschale Festlegungen über Umfang, Art und Zweck der DV nicht aus. Bei Nr. 3 empfahl Gosche eine Maximalliste zum Ankreuzen, die Bezugnahme auf bereits bestehende Sicherheitskonzepte des Auftragnehmers oder auch die Bezugnahme auf anerkannte Datenschutz Zertifizierungen (zum Beispiel Gütesiegel ULD, Trusted Shop). Man solle sich außerdem das Recht vorbehalten, Schutzmaßnahmen anpassen zu können. Bei Nr. 7 seien individuell abgestufte Kontrollkonzepte empfehlenswert. Eigene Prüfungen des Auftraggebers vor Ort sieht Gosche nicht immer als zwingend, aber in vielen Fällen als ratsam an. Unter Umständen sei auch die Einholung von Bestätigungen des betrieblichen Datenschutzbeauftragten des Auftragnehmers möglich. Sämtliche Kontrollen des Auftraggebers sollten gewissenhaft und ernsthaft dokumentiert werden.

Dorothee Freise, Schufa Holding, war der Auffassung, dass sich die Pflicht des Auftragnehmers zur novellierungsbedingten Vertragsanpassung aus § 313 Abs. 1 Bürgerliches Gesetzbuch ergebe (wo-

bei jede Partei die Kosten selbst zu tragen habe). Für die Definition von „Wartung“ könne auf § 3 Abs. 3 Nr. 5 des Brandenburgischen Datenschutzgesetzes zurückgegriffen werden. Ob Gewährleistungsfälle unter den Anwendungsbereich von § 11 Abs. 5 BDSG fallen, sei bisher offen. Dr. Uwe Hajda erläuterte die Umsetzungserfordernisse. Rechtsabteilung und Datenschutzbeauftragter müssten sich in das Vertragsmanagement einbringen. Den Fachabteilungen sollten in großen Unternehmen oder Unternehmensverbänden vernünftige Entscheidungs routinen und Handlungsempfehlungen an die Hand gegeben werden.

Der Tagungsband, der auch die weiteren Schwerpunkte der diesjährigen Herbstakademie (Softwarevertrags-, Immaterialgüter- und Internetrecht) abdeckt, ist bereits im Oldenburg-Verlag erschienen (858 Seiten, ISBN-13 978-3-939704-50-8, EUR 49,80).



Internet:

www.dsri.de

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_de.pdf

www.cnil.fr/fileadmin/documents/en/D-Discovery_EN.pdf

www.theseconconference.org

www.olwir.de (Rubrik Neuerscheinungen)

Stichworte: DSRI, Herbstakademie, Beschäftigtendatenschutz, E-Discovery, Auftragsdatenverarbeitung

Unzulässige Weitergabe von Patientendaten durch Hausärzte

Eigentlich erscheint es ganz „normal“: Die Hausärzte wollen sich die Abrechnung ihrer Tätigkeit vereinfachen und damit Dienstleister beauftragen. Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) hat in einer Verfügung dem Hausärzterverband Schleswig-Holstein e.V. (HÄV SH) unter Androhung eines Zwangsgeldes in Höhe von EUR 30.000,- untersagt, gemäß dem zwischen der AOK Schleswig-Holstein, dem HÄV SH und Dienstleistern abgeschlossenen Vertrag von eingeschriebenen Hausärzten stammende Patientendaten weiterzugeben oder diese selbst zu nutzen. Die sofortige Vollziehung dieser Verfügung wurde angeordnet.

Von **HOLGER KOCH, Mixdorf.**

Der Vertrag zwischen den im Hausärzterverband zusammengeschlossenen Ärzten, der AOK und

bestimmten Abrechnungsdienstleistern wurde von der Datenschutzbehörde in Schleswig-Holstein als datenschutzrechtlich unzulässig beanstandet und bei Einführung des geplanten Verfahrens Bußgeld angedroht. Dieses Verfahren ist nach den Angaben des ULD so gestaltet, dass die Hausärzte keine Möglichkeit der Kontrolle über die Weitergabe von Patientendaten durch ihr Praxissystem mehr hätten und dass der Hausärzterverband Kenntnis von Abrechnungsdaten erhält. Es muss danach auf den Praxissystemen eine Software gemäß den Vorgaben des Hausärzterverbandes installiert werden, ohne dass die Hausärzte letztlich wissen, welche Aktivitäten diese Software durchführt. Das würde natürlich das Auftragsverhältnis auf den Kopf stellen. Der einzelne Arzt muss den Datenschutz und die ärztliche Schweigepflicht sicherstellen. Und dazu bedarf es der Kenntnis über die Funktionalität der eingesetzten Software. Die Frage ist, ob ein ein-