II. Stellungnahme der EU-Kommission zum Entwurf der BNetzA

Die *EU-Kommission* hat sich zu dem Konsolidierungsentwurf, welcher von der endgültigen Regulierungsverfügung grundsätzlich nicht abweicht, in ungewohnt offener Weise geäußert (*EU-Kommission*, Stellungnahme gem. Art. 7 Abs. 3 der RL 2002/21/EG, K(2011)1338).

1. Zugangsverpflichtung

Die *Kommission* kritisierte dabei den Umstand, dass die Zugangsverpflichtung hinsichtlich des Punkts, an dem der Netzzugang gewährt werden soll, von der jeweiligen Netzstruktur abhängig gemacht wird. Auf diese Weise bestehe die Gefahr, dass dadurch die Wahl hinsichtlich der Technik zum weiteren Netzausbau beeinflusst wird. Unter Hinweis auf die NGA-Empfehlung forderte die *Kommission* die *BNetzA* auf, eine klare und technologieneutrale Zugangsverpflichtung zu formulieren, die einen Zugang an dem aus Sicht der *Kommission* „zweckmäßigsten" Punkt, dem MPoP (Metropolitan Point of Presence) oder an einem vergleichbar geeigneten Verteilerpunkt anordne (*EU-Kommission*, S. 5).

2. ex post-Regulierung

Weiterhin bezweifelt die *EU-Kommission*, dass durch eine nachträgliche Entgeltkontrolle den auf dem Markt festgestellten Wettbewerbsproblemen adäquat begegnet werden könne (*EU-Kommission*, S. 6). Zugangsentgelte müssten sich an den tatsächlichen Kosten orientieren und dabei transparent sein, so die *Kommission*. Ähnlich hatte die *Kommission* schon in einem anderen Verfahren argumentiert (Breitbandzugang auf Vorleistungsebene, DE/2010/1116). Mit der gewählten nachträglichen Entgeltkontrolle sei nicht die notwendige Rechtssicherheit zu erreichen, wodurch gerade ein vertikal integriertes Unternehmen mit beträchtlicher Marktmacht tendenziell begünstigt würde (*EU-Kommission*, a.a.O.).

III. Fazit

Die *BNetzA* hat trotz der Kritik der *EU-Kommission* an ihrer Auffassung festgehalten. Beim entbündelten Zugang zu Glasfaserinfrastrukturen der *Telekom Deutschland GmbH* hält die *BNetzA* die Verpflichtung in Abhängigkeit der jeweilig benutzten Technologie recht offen und die Glasfaser-TAL wird in ihrer Regulierungsverfügung lediglich einer ex post-Kontrolle unterworfen. Art. 7 Abs. 7 RahmenRL, zuletzt geändert durch die RL 2009/140/EG, sieht vor, dass die nationalen Regulierungsbehörden den Stellungnahmen der *EU-Kommission* „weitestgehend Rechnung" zu tragen haben, untersagt den nationalen Regulierungsbehörden jedoch nicht grundsätzlich, sich über diese hinwegzusetzen.

Welche Auswirkungen die nun getroffenen Verpflichtungen hinsichtlich eines entbündelten Zugangs zur Glasfaser-TAL auf den weiteren Netzausbau haben wird und ob die von der *BNetzA* angenommene „disziplinierende Wirkung" der ex ante-regulierten Kupfer-TAL auf die Entgelte der Glasfaser-TAL tatsächlich eintritt, bleibt abzuwarten. Die Wettbewerber der *Telekom Deutschland GmbH* dürften diese Entwicklung genauestens verfolgen.

Marc Schramm
ist Leiter Recht & Regulierung beim BREKO – Bundesverband Breitbandkommunikation e.V. in Bonn. Der Beitrag gibt ausschließlich die persönliche Meinung des Autors wieder.

Axel Spies Neues Tool im Datenschutz: „Prividor" als Einfallstor für Abmahnungen?

MMR-Aktuell 2011, 316402

Im Beck-Blog (www.blog.beck.de) gab es kürzlich eine recht intensive Diskussion zum Thema Abmahnungen bei der Verletzung von Datenschutzrechten, die nachfolgend kurz zusammengefasst wird.

1. Hintergrund

Der Bundesdatenschutzbeauftragte *Schaar* hat am 25.3.2011 den vom *Fraunhofer-Institut für Sichere Informationstechnologie* (*SIT*) entwickelten „Privacy Violation Detector" (Prividor) vorgestellt. Prividor soll automatisiert erkennen, ob

- „Tracking", also das heimliche Ausspähen des Surfverhaltens, vorliegt,
- die Liste der besuchten Webseiten, also der Browserverlauf, ausgelesen wird,
- problematische Onlinedienste, die das Programm anhand einer Blacklist erkennt, verwendet werden.

Des Weiteren soll Prividor

- die Verwendung unverschlüsselter Formulare aufzeichnen und
- die Ergebnisse in Übersichten aufbereiten, die vorerst den Aufsichtsbehörden als Basis zum Einschreiten dienen sollen.

Zunächst soll Prividor nur bei Internetauftritten eingesetzt werden, die dem Aufgabenbereich des *Bundesbeauftragten für den Datenschutz und die Informationsfreiheit* (*BfDI*) zufallen. Dies umfasst die Internetauftritte aller Bundesbehörden sowie der Post- und TK-Unternehmen. Nach einer Testphase soll das Programm auch den Landesdatenschutzbehörden zur Verfügung gestellt werden. Als möglichen dritten Schritt sieht *Schaar* die Bereitstellung von Prividor als frei zugängliches Programm im Internet (Open Source Software).

Durch die Bereitstellung von Prividor im Internet wird jedoch befürchtet, dass dadurch „Abmahnanwälten" die Verfolgung von Rechtsverstößen auf Internetseiten erheblich erleichtert wird und dadurch eine neue Abmahnwelle bei Datenschutzverstößen auf die Betreiber von Internetseiten zukommt. Der *BfDI* sieht in einem Interview mit dem Online-Magazin Heise allerdings keinen Grund, der gegen Prividor oder dessen Bereitstellung spreche. Jeder, so *Schaar*, hätte das Recht zu prüfen, ob bestimmte Vorgaben eingehalten werden. Unternehmen und öffentliche Stellen müssten dafür sorgen, dass sie gesetzeskonform handeln.

2. Diskussion im Blog

a) Datenschutzregelungen als „Marktverhaltensregeln"

Die Diskussion im Blog kreiste vor allem um die Frage, ob die Regelungen des BDSG Marktverhaltensregeln i.S.d. UWG darstellen. Hierzu wurde angemerkt, dass die wettbewerbsrechtliche Bedeutung das Datenschutzes seit etwa 30 Jahren umstritten sei. Es gebe etwa ein Dutzend obergerichtlicher Entscheidungen mit leichtem Übergewicht pro Lauterkeitsverstoß. Auch der *I. Zivilsenat des BGH* habe sich 1992 für die wettbewerbsrechtliche Bedeutung des Datenschutzes ausgesprochen. Zu Zeiten des § 1 UWG a.F. habe man sich bei wettbewerbsneutralen Normen auch auf die besondere Bedeutung des Datenschutzes sowie auf einen Vorsprung durch gezielten Rechtsbruch berufen können, was

seit der Einführung von § 4 Nr. 11 UWG ausgeschlossen sei.
Es wurde weiterhin angemerkt, dass Datenschutzregelungen Marktverhaltensregelungen gem. § 4 Nr. 11 UWG oder Verbraucherschutzbestimmungen nach § 2 Abs. 1 UKlaG zumindest dann seien, wenn sie über den Schutz des Rechts auf informationelle Selbstbestimmung hinaus auch das Ziel hätten, für ausgewogene rechtliche Marktverhältnisse zu sorgen. Sie dürfen also nicht nur den betriebsinternen Bereich umfassen, sondern Fälle betreffen, in denen die Daten als Ware Bedeutung hätten. Genannt wurden insbesondere § 29 BDSG oder Fälle der Werbung oder Marktforschung (mit Verweis auf *OLG Köln* MMR 2009, 845 m. Anm. *Haas/Stallberg* – Kundenrückgewinnungsschreiben; *Köhler*, zu § 4 Nr. 11 UWG). Diskutiert wurde in diesem Zusammenhang eine Entscheidung des *OLG Stuttgart* (MMR 2007, 437), die die Anwendung des § 4 Nr. 11 UWG bei einem Verstoß gegen § 28 BDSG bejaht hat. In dem konkreten Fall sei nach Ansicht des *Gerichts* der Wettbewerbsverstoß mehr als ein „bloßer Reflex" des Verstoßes gegen die Datenschutzbestimmungen (unzulässige Weitergabe von Kundendaten einschließlich Bankverbindung). Auch nach Ansicht des *OLG Stuttgart* ist die Anwendbarkeit dann gegeben, „wenn der Empfänger, der um die rechtswidrige Weitergabe derselben [Daten] weiß, diese Daten zu Werbezwecken oder in sonstiger Weise wettbewerbserheblich verwenden will und verwendet." (a.a.O., S. 438).

b) Abmahnunwesen

Uneinig waren sich die Diskussionsteilnehmer darüber, ob massenhafte Abmahnungen im Datenschutzsektor ein Segen oder ein Fluch seien. Ein Teilnehmer der Diskussion meinte, der „Abmahnwahn in Deutschland" treffe im Wettbewerbsrecht immer nur kleine und mittelständische Unternehmen hart, denn sie müssten „die Zeche für eine praxisferne Gesetzeslage und – leider auch – Rechtsprechung zahlen." Durch Abmahnungen sei der Wettbewerb kein bisschen sauberer geworden, Abmahnkosten trügen nur zu steigenden Verbraucherpreisen bei. Andere Teilnehmer der Diskussion führten an, dass es „offensichtlich" sei, „dass eine Vielzahl der Internetauftritte gegen gesetzliche Vorgaben verstoßen. Hierbei handele es sich meist um Datenschutzverstöße oder um fehlerhafte Impressen." In diesen Fällen, so diese Gruppe, müssen auch Abmahnungen möglich sein.

Dr. Axel Spies
ist Rechtsanwalt in der Kanzlei Bingham McCutchen in Washington DC und Mitherausgeber der MMR.

Tim Wybitul BAG: Betriebsratsmitglied kann Datenschutzbeauftragter sein – Hohe Anforderungen an Kündigung des betrieblichen Datenschutzbeauftragten

MMR-Aktuell 2011, 316297

Das BDSG und die Aufsichtsbehörden für den Datenschutz richten an die Fachkunde und Zuverlässigkeit von betrieblichen Datenschutzbeauftragten hohe Anforderungen. Erfüllt der Datenschutzbeauftragte diese Anforderungen nicht, drohen schlimmstenfalls Bußgelder von bis zu € 50.000,–. Allerdings ist es für Unternehmen schwer, sich von einem einmal bestellten Datenschutzbeauftragten zu trennen, wie ein aktuell vom *BAG* (MMR-Aktuell 2011, 315976) entschiedener Fall zeigt. Das *Gericht* hat in diesem Zusammenhang zudem entschieden, dass ein Betriebsratsmitglied grundsätzlich hinreichend unabhängig ist, um als Datenschutzbeauftragter tätig zu sein.
Das *BAG* hatte am 23.3.2011 über die Kündigung einer Datenschutzbeauftragten zu entscheiden. Die Klägerin war seit 1981 im Bereich der Fluggastabfertigung beschäftigt. 1992 wurde sie zur Datenschutzbeauftragen im Unternehmen ihres Arbeitgebers und bei einer Tochtergesellschaft bestellt. 30% ihrer Arbeitszeit verbrachte sie mit ihren Aufgaben als Datenschutzbeauftragte. Seit 1994 war die Klägerin zudem Mitglied des Betriebsrats ihres Arbeitgebers. Im Februar 2008 beschloss die Geschäftsleitung des Arbeitgebers, einen externen Datenschutzbeauftragten zu bestellen. Dieser sollte beim Arbeitgeber und bei dessen Tochtergesellschaften künftig einheitlich auf die Einhaltung des BDSG und anderer Datenschutzgesetze hinwirken. Die Arbeitgeberin widerrief daraufhin die Bestellung der Beklagten als Datenschutzbeauftragte und sprach bezüglich der 30%-igen Tätigkeit als Datenschutzbeauftragte eine Teilkündigung aus. Mit einer solchen Teilkündigung kann der Arbeitgeber den auf die Beschäftigung als Datenschutzbeauftragter bezogenen Teil des Arbeitsverhältnisses abändern, falls der Widerruf der Bestellung wirksam ist. Die zusätzliche Aufgabe im Rahmen des Arbeitsverhältnisses als Datenschutzbeauftragte fällt dann durch die Teilkündigung weg. Nach dem Willen des Arbeitgebers sollte die Klägerin künftig daher wieder in Vollzeit in der Fluggastabfertigung arbeiten. Die Vorinstanzen hatten der Klage der Datenschutzbeauftragten stattgegeben. Auch das *BAG* gab der Klägerin Recht.

1. Widerruf der Bestellung zum Datenschutzbeauftragten nur aus wichtigem Grund

Die gesetzlichen Regelungen in § 4f Abs. 3 Satz 4 BDSG und § 626 BGB gewähren Datenschutzbeauftragten einen besonderen Abberufungsschutz. Damit soll ihre Unabhängigkeit und die weisungsfreie Ausübung des Amts gestärkt werden (vgl. *Wybitul*, Hdb. Datenschutz im Unternehmen, 1. Aufl. 2011, Rdnr. 261). Die Bestellung zum Beauftragten für den Datenschutz kann nur aus wichtigem Grund widerrufen werden. Die Maßstäbe für das Vorliegen eines solchen wichtigen Grundes sind dieselben wie bei einer fristlosen Kündigung. Eine Abberufung aus wichtigem Grund ist nur möglich, wenn eine Fortsetzung des Rechtsverhältnisses für den Arbeitgeber unzumutbar ist. Beispiele wären etwa schwerwiegende Verletzungen der Informations- und Kontrollaufgaben des Datenschutzbeauftragten oder die unberechtigte Weitergabe vertraulicher Informationen (vgl. *Scheja*, in: Taeger/Gabel, BDSG, 1. Aufl. 2010, § 4f Rdnr. 42). Weder die Entscheidung des Arbeitgebers, zukünftig die Aufgaben eines Beauftragten für den Datenschutz durch einen externen Dritten wahrnehmen zu lassen, noch die Mitgliedschaft der Datenschutzbeauftragten im Betriebsrat stellen nach Ansicht des *BAG* einen solchen wichtigen Grund für den Widerruf dar. Als Folge des unwirksamen Wider-