Bundesverband Glasfaseranschluss e. V.

**PRESSEMITTEILUNG**

# „Wertvoll für die Unternehmen, wichtig für die Kunden“

## BUGLAS-Infothek zu Herausforderungen für Datenschutzbeauftragte in Telekommunikationsunternehmen

**Köln, 2. Juni 2015.** Der Datenschutz genießt in Deutschland einen hohen Stellenwert. Durch die dynamische Entwicklung auf dem Digitalmarkt werden die Herausforderungen für Telekommunikationsunternehmen auf diesem Gebiet immer komplexer. „Ich fühle mich häufig wie eine unterschätzte Spezies im Firmengeflecht“, beschreibt ein Teilnehmer seine praktische Arbeit als Datenschutzbeauftragter im Spannungsfeld zwischen Schutzbedürfnissen, Umsetzbarkeit und Wirtschaftlichkeit. Im Rahmen einer Infothek beleuchtete der Bundesverband Glasfaseranschluss (BUGLAS) diese und weitere Herausforderungen für die betrieblichen Wächter der Datensicherheit gemeinsam mit der Düsseldorfer Kanzlei JUCONOMY aus verschiedenen Blickwinkeln. Gleich zu Beginn wird mit der Aussage der Knackpunkt für viele Betriebe deutlich: „Die Anforderungen an den Datenschutzbeauftragten sind sehr umfangreich und erfordern ein hohes Maß an rechtlichem, technischem und organisatorischem Wissen“, berichtet BUGLAS-Justiziarin Astrid Braken. Daher biete der Verband bewusst zusätzliche Unterstützung von Experten und die Möglichkeit zum fachlichen Austausch mit solchen Veranstaltungsformaten an. Denn die vielfältigen datenschutzrechtlichen Fallstricke in der Praxis seien eben ein „Dauerbrenner“, wie nicht nur zahlreiche Anfragen von Mitgliedsunternehmen belegten.

Martin Huerkamp kann die Sichtweise als Datenschutz- und Compliance-Beauftragter des Kölner Telekommunikationsanbieters NetCologne bestätigen: Das „enge Regelungskorsett“ mache es zum Teil kompliziert, berechtigte Wünsche aus den Fachabteilungen zu erfüllen. Beispielsweise stecke man schon in einem Dilemma, wenn das Unternehmen ein verbessertes Serviceangebot für Kunden bieten möchte, dazu aber auf konzerninterne Daten zugreifen müsste. „Dann bin ich derjenige, der die Umsetzung solch guter Ideen ermöglicht, ohne dass es rechtliche Probleme gibt.“ Daher sei seine Arbeit gleichermaßen „wichtig für die Verbraucher und wertvoll für das Unternehmen“. Das Aufgabengebiet von Herrn Huerkamp umfasst

nicht nur datenschutzrelevante Themen. Seine Expertise ist ebenso für den Umgang mit besonders schützenswerten Kommunikationsdaten, insbesondere im Bereich der Telekommunikationsüberwachung, gefragt, da diese besonderen rechtlichen Rahmenbedingungen genügen müssen. „Die engen Vorgaben aus Berlin und Brüssel sind da oft nur schwer nachzuvollziehen."

Rechtsanwalt Dr. Jens Eckhardt von der Kanzlei JUCONOMY versteht als Spezialist für Telekommunikationsrecht diese Welt zwar besser, räumt aber ebenfalls ein, dass die Umsetzung für Datenschutzverantwortliche in den Firmen „in der Praxis häufig problematisch" sei. In diesem Zusammenhang würden besonders die Anforderungen bei der Auftragsdatenverarbeitung unterschätzt, die vor allem Cloud-Dienstleister träfen. Anbieter würden nach seinen Erfahrungen gerne versuchen, durch Auslagerungsprozesse die Risiken zu minimieren. „Cloud Computing bringt nicht die gewünschten Einspareffekte, wenn der Datenschutz nicht frühzeitig und als Bestandteil der Auslagerungsstrategie in die Betrachtung einbezogen wird", warnt der Fachanwalt für IT-Recht. Denn gerade für die Auftragsdatenverarbeitung sehe das deutsche Datenschutzrecht vergleichsweise strikte Vorgaben vor. „Nur wenn die datenschutzrechtlichen Hausaufgaben gemacht sind, kann sich das Potenzial von Cloud Services vollständig entfalten."

Aus der „Not eine Tugend" zu machen, empfiehlt entsprechend IT-Berater und Compliance-Experte Thomas Floß. Besonders eigne sich dazu das Verfahrensverzeichnis, das ohnehin gesetzlich vorgeschrieben sei. Dies sei ein „absolutes Muss" für alle eingesetzten Verarbeitungen von Daten - unabhängig von der Unternehmensgröße und bereits vorhandenen Datenschutzbeauftragten. „Leider wissen das die wenigsten Selbstständigen." Generell sei es ratsam, vor allem auf Datenvermeidung zu setzen: „Wenn man alle Prozesse erfasst, die mit internen und externen Informationen zu tun haben, kann das helfen." So ließen sich mit der Pflichtaufgabe im Endeffekt sogar Kosten sparen. Zudem sei man „gerüstet, wenn der Ernstfall eintritt".

Was genau der Ernstfall bedeutet und für die Unternehmen dann zu tun ist, schildert Dirk Hensel von der Dienststelle der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) dem Fachpublikum. „Ob der Mitarbeiter sich mit den Daten aus dem Staub macht, Systeme versehentlich ungesichert im Netz stehen oder Hacker es auf die Server

abgesehen hatten – schnelles und sorgfältiges Handeln ist dann gefragt.“ Für eine sogenannte Erstmeldung an die Behörden nach 109a TKG hätten Firmen nur 24 Stunden Zeit. „Viele Verantwortliche haben das leider gar nicht auf dem Radar“, bemängelt Hensel. Dabei bestehe durchaus die Möglichkeit, zunächst den Vorfall zu melden und wichtige Details nachzureichen, um die Frist zu wahren. Hensel betont, dass bei aller Kritik an manchen Vorgaben der Schutz der Betroffenen von Datenschutzpannen im Vordergrund stehe. Die Aufsichtsbehörden fungieren hier lediglich als „objektive Kontrollinstanz“. Gerne stehe er für Rückfragen bereit, wenn Anbieter sich bei einer Sachfrage unsicher sind. „Wir arbeiten Hand in Hand, wir sind nicht der Gegenspieler.“ Negative Konsequenzen müsse nur fürchten, wer das Thema „mutwillig auf die leichte Schulter“ nehme.

Den Datenschutz ernst zu nehmen, rät auch der Brüsseler Verbindungsanwalt der BUGLAS, Dr. Alexander Benczek, der die regulatorischen und politischen Entwicklungen auf EU-Ebene im Blick hat: „Da kommt noch vieles auf IT-Hersteller und Datenverarbeiter zu, was Ressourcen binden wird.“ Dies gelte in besonderem Maße für EU-Mitgliedstaaten, in denen die Datenschutzstandards geringer sind als in Deutschland. So werde im Augenblick bei den Institutionen vorrangig daran gearbeitet, den „Flickenteppich“ an nationalen Regelungen zum Datenschutz auf einem hohen Niveau zu vereinheitlichen und bestehende datenschutzrechtliche Vorgaben aus dem Jahr 1995 an die technisch bedingten Entwicklungen des 21. Jahrhunderts anzupassen, wie die Verarbeitung von Daten aus sozialen Netzwerken oder aus automatisierten M2M-Verbindungen. Eine Neuigkeit lässt die Unternehmensvertreter besonders aufhorchen: Die Europäische Kommission plant, bei Datenschutzvergehen Sanktionen in Höhe von bis zu zwei Prozent des weltweiten Jahresumsatzes zu verhängen. Im Europäischen Parlament sind sogar bis zu fünf Prozent im Gespräch. Auch wenn es als unwahrscheinlich gilt, dass die Aufsichtsbehörden diesen Rahmen voll ausschöpfen: „Bei wem der Datenschutz bislang keinen hohen Stellenwert hatte, sollte nun definitiv umdenken“, empfiehlt Benczek.

Der BUGLAS beleuchtet mit seinem Infothek-Veranstaltungsformat seit Sommer 2013 wichtige übergreifende Themen mit Auswirkungen für die Glasfaserbranche detailliert aus verschiedenen Blickwinkeln. Erfolgreiche Fachtagungen wurden beispielsweise zur Vorratsdatenspeicherung, SEPA-Einführung, Public WLAN, Verbraucherschutzvorgaben im TKG oder IP-TV durchgeführt.

Bundesverband Glasfaseranschluss e. V.

**Über den Bundesverband Glasfaseranschluss e. V. (BUGLAS):**

Im BUGLAS sind die Unternehmen zusammengeschlossen, die in Deutschland hochleistungsfähige Glasfasernetze mit dedizierten Bandbreiten bis in den Gigabit-Bereich errichten und betreiben und bis Ende 2014 schon über 1,4 Millionen Haushalte direkt mit Glasfaser angeschlossen haben. Der Verband tritt für einen investitionsfreundlichen ordnungspolitischen Rahmen und das Prinzip des Infrastrukturwettbewerbs ein.

**Pressekontakt:**

Bundesverband Glasfaseranschluss e. V.
Wolfgang Heer, Geschäftsführer
Bahnhofstraße 11, 51143 Köln
Tel.: +49 2203 20210-10
Fax: +49 2203 20210-88
E-Mail: heer@buglas.de
Internet: http://www.buglas.de