

Rechtliche Stolpersteine

Über technische Fragen hinaus hat sich der 4. Österreichische IT-Sicherheitstag am 7. November 2007 in Klagenfurt mit rechtlichen Problemen der Informationstechnologie beschäftigt.

Der Webauftritt ist für Unternehmen längst nichts mehr Außergewöhnliches“, stellte Dr. Sonja Janisch von der Universität Salzburg fest. „Doch gibt es rechtliche Stolpersteine beim Webauftritt, die zu Rechtsstreitigkeiten führen können.“ Regelungen zur Frage, welche Inhalte eine Website aufweisen muss, finden sich in verschiedenen Gesetzen. Als eines davon kommt das Mediengesetz in Betracht. Seit der Mediengesetz-Novelle 2005 gilt eine Website als periodisches, elektronisches Medium. Anders als bei einem Newsletter (wiederkehrendes elektronisches Medium; § 1 Abs. 5a lit c MedienG) ist für eine Website ein Impressum nicht erforderlich (§ 24 Abs. 3 MedienG).

Den Medieninhaber treffen aber medienrechtliche Offenlegungspflichten, deren Umfang davon abhängt, ob die Site meinungsbeeinflussend ist oder nicht. Weist die Site einen über die Darstellung des persönlichen Lebensbereichs oder die Präsentation des Medieninhabers hinausgehenden Informationsgehalt auf, der geeignet ist, die öffentliche Meinungsbildung zu beeinflussen, ist der Medieninhaber anzugeben mit Namen oder Firma, mit Unternehmensgegenstand, mit Wohnort, Sitz oder Niederlassung und mit Art und Höhe der Beteiligung (§ 25 Abs. 2 MedienG). Diese Angaben sind ständig leicht und unmittelbar auffindbar zur Verfügung zu stellen (§ 25 Abs. 1 MedienG). Bei Websites, die nicht meinungsbeeinflussend sind, genügen die Angabe des Namens oder der Firma, gegebenenfalls des Unternehmensgegenstandes sowie des Wohnorts oder des Sitzes des Medieninhabers (§ 25 Abs. 5 MedienG).



Bei einem kommerziellen Webauftritt sind umfangreiche Informationspflichten nach dem E-Commerce-Gesetz zu beachten, die gemeinsam mit den Angaben zur Offenlegung zur Verfügung gestellt werden können.

einflussend sind, genügen die Angabe des Namens oder der Firma, gegebenenfalls des Unternehmensgegenstandes sowie des Wohnorts oder des Sitzes des Medieninhabers (§ 25 Abs. 5 MedienG).

Bei einem kommerziellen Webauftritt sind umfangreiche Informationspflichten nach dem E-Commerce-Gesetz (ECG) zu beachten, die gemeinsam mit den Angaben zur Offenlegung zur Verfügung gestellt werden können (§ 25 Abs. 1 MedienG). Der Diensteanbieter (§ 3 Z 2 ECG) hat nach § 5 Abs. 1 ECG den Nutzern

ständig zumindest folgende Informationen leicht und unmittelbar zur Verfügung zu stellen:

Seinen Namen oder seine Firma (Z 1); die Anschrift, unter der er niedergelassen ist (Z 2); Angaben, auf Grund deren die Nutzer mit ihm rasch und unmittelbar in Verbindung treten können, einschließlich seiner elektronischen Postadresse (Z 3); sofern vorhanden, die Firmenbuchnummer und das Firmenbuchgericht (Z 4); soweit die Tätigkeit einer behördlichen Aufsicht unterliegt, die für ihn zuständige Aufsichtsbehörde (Z 5); den Berufsverband (Z

6) und, sofern vorhanden, die Umsatzsteuer-Identifikationsnummer (Z 7).

Preise sind so auszuzeichnen, dass sie ein durchschnittlich aufmerksamer Betrachter leicht lesen und zuordnen kann. Es muss eindeutig erkennbar sein, ob die Preise einschließlich der Umsatzsteuer sowie aller sonstigen Abgaben und Zuschläge ausgezeichnet sind (Bruttopreise) oder nicht. Darüber hinaus ist auch anzugeben, ob Versandkosten enthalten sind (§ 5 Abs. 2 ECG).

Die Betreiber von Webshops haben gemäß § 9 Abs. 1 ECG einen Nutzer vor Abgabe seiner Vertragserklärung klar, verständlich und eindeutig zu informieren: Über die einzelnen technischen Schritte, die zu seiner Vertragserklärung und zum Vertragsabschluss führen (Z 1); den Umstand, ob der Vertragstext nach Vertragsabschluss vom Diensteanbieter gespeichert wird sowie gegebenenfalls den Zugang zu einem solchen Vertragstext (Z 2); die technischen Mittel zur Erkennung und Berichtigung von Eingabefehlern vor Abgabe der Vertragserklärung (Z 3) sowie die Sprachen, in denen der Vertrag abgeschlossen werden kann (Z 4).

Wenn einem Verbraucher eine Bestellmöglichkeit eröffnet wird, müssen ihm die in den §§ 5c und 5d des Konsumentenschutzgesetzes angeführten Informationen rechtzeitig vor Vertragsabschluss zur Verfügung stehen. Letztlich verpflichtet § 14 Unternehmensgesetz-

buch (UGB) alle ins Firmenbuch eingetragenen Unternehmen auf ihren Webseiten unter anderem die Firma, die Rechtsform, den Sitz und die Firmenbuchnummer des Unternehmers sowie das Firmenbuchgericht anzugeben. Verletzungen dieser Pflichten können verwaltungsstrafrechtliche Folgen haben (Mediengesetz, ECG) oder zivilrechtliche Konsequenzen, wie Schadenersatzansprüche oder wettbewerbsrechtliche Unterlassungsklagen nach sich ziehen. Bei Fernabsatzverträgen kann sich die Rücktrittsfrist des Verbrauchers verlängern.

Unzulässige Inhalte. Das Web mit seiner unerschöpflich scheinenden Fülle an Texten, Schriftarten, Grafiken, Bildern, Landkarten, Audio- und Videoangeboten verleitet dazu, sich dieses Material zu Nutze zu machen. Dabei handelt es sich allerdings um Werke im Sinn des Urheberrechtsgesetzes, zu deren Verwendung die Zustimmung des Urhebers erforderlich ist. Dieser hat gegen einen Verletzer, was in der Praxis am häufigsten geltend gemacht wird, unter anderem einen Unterlassungsanspruch, der

nicht voraussetzt, dass der Rechteverletzer von dem Eingriff in das Urheberrecht wusste oder dass ihn sonst ein Verschulden trifft, und der auch nicht dadurch beseitigt wird, dass das dem Schutz unterliegende Werk sofort entfernt wird. Bei Verschulden an der Verletzung sind nach dem Urheberrechtsgesetz auch weitere zivil- und strafrechtliche Konsequenzen möglich.

Bei Suchmaschinen ist es möglich, sich in den Vordergrund zu schieben, indem man die *Metatags* seiner Website mit häufig angefragten Suchbegriffen oder bekannten Markennamen versieht, mit dem Ziel, dass bei Anfragen die eigene Website als Treffer ausgeworfen wird. Diese *Metatags* sind für den Betrachter der Website – ohne ausdrücklichen Aufruf des Quellcodes – nicht sichtbar, werden aber von den Suchmaschinen erfasst. Das stellt unlauteren Wettbewerb dar oder auch eine Verletzung von Markenrechten.

Dass man für eigene Inhalte auf Websites verantwortlich ist, liegt auf der Hand. Man kann allerdings fremde Informationen als seine eigenen darstellen, und ist dann, trotz der sons-

ebenfalls jährlich abgehaltene D-A-CH-Security bietet Deutschland, Österreich und der Schweiz eine interdisziplinäre Übersicht zum aktuellen Stand der IT-Sicherheit in Industrie, Dienstleistung, Verwaltung und Wissenschaft, mit dem Schwerpunkt Forschung und Entwicklung sowie neuer Technologien und sich daraus ergebender Produktentwicklungen.

Die D-A-CH-Security 2008 findet am 24. und 25. Juni 2008 in Berlin statt.

SYSSEC

IT-Sicherheitstag

Seit 2004 hält die Forschungsgruppe System-sicherheit der Universität Klagenfurt (www.syssec.at) unter Univ.-Prof. Dr. Patrick Horster in jährlichem Abstand die Österreichischen IT-Sicherheitstage ab.

Deren Ziel es ist, vor allem für kleine und mittlere Unternehmen praxisnahe und wirtschaftlich vertretbare Lösungen für IT-Sicherheit vorzustellen. Die

ORTHOPÄDIE- UND MASSSCHUHMACHERMEISTER THOMAS DUNZINGER

15., Mariahilfer Straße 217a
Tel.: 892 20 18, Fax: 897 58 17
office@dunzinger-schuh.at
www.dunzinger-schuh.at

Geschäftszeiten:
Mo-Fr: 9.00-12.00 und 14.30-18.00
Sa: nach tel. Vereinbarung
Orthopädie gegen Voranmeldung

- Orthopädische Schuhe
- Innenschuhe
- orthop. Schuhzurichtung
- Modell- und Sporteinlagen
- Propriozeptive Einlagen
- Diabetikerversorgung und -schuhe
- Maßschuhe, Maßreitstiefel
- Sportbandagen
- Kompressionsstrümpfe
- Therapie- und Gesundheitsschuhe
- Fachberatung bei Fußbeschwerden



**Vertragspartner aller Krankenkassen
Hausbesuche**

Ihr Partner im Schweißen und Schneiden



Schweiß- und Schneidausrüstung

Schweißautomaten

Schweißzusätze

Schneidsysteme

Dirmhirngasse 110
1235 Wien-Liesing

Tel.: 01 / 888 25 11
Telefax: 01 / 888 25 11-85
ESAB im Internet: www.esab.at
info@esab.co.at

tigen Privilegierung nach § 17 Abs. 1 ECG, auch für diese Inhalte verantwortlich (§ 17 Abs. 2 ECG).

Online-Gästebuch. Ähnlich verhält es sich bei Eintragungen, die Nutzer direkt und online in einem über Internet zur Verfügung gestellten „Gästebuch“ als eine Art Leserbrief machen können. Der Betreiber eines solchen Gästebuchs ist, wie der OGH in seinem Urteil vom 21. Dezember 2006, 6 Ob 178/04a festgestellt hat, als „Host-Provider“ im Sinn des § 16 ECG anzusehen. Dieser ist nach § 18 Abs. 1 ECG zwar nicht verpflichtet, die von ihm gespeicherten, übermittelten oder zugänglich gemachten Informationen zu überwachen oder von sich aus nach Umständen zu forschen, die auf rechtswidrige Tätigkeiten hinweisen, doch der Abschluss der Verantwortlichkeit nach § 16 Abs. 1 ECG schließt lediglich eine allfällige Schadenersatzhaftung und die strafrechtliche Verantwortlichkeit aus, nicht jedoch verschuldensunabhängige zivilrechtliche Unterlassungsansprüche.

Demnach kann derjenige, der ein Online-Gästebuch im Internet betreibt, als Verbreiter auf Unterlassung rechtswidriger Inhalte in Anspruch genommen werden. Es besteht zwar schon aus Gründen der Freiheit der Meinungsäußerung (Art 10 EMRK; Art 13 StGG) keine allgemeine Verpflichtung zu einer Kontrolle der Beiträge, doch trifft den Betreiber die Verpflichtung, bei Bekanntwerden rechtswidriger Inhalte die Beiträge zu entfernen. Zudem ist eine besondere Kontrollpflicht zumutbar, dass sich weitere rufschädigende und beleidigende Eintragungen nicht wiederholen, insbesondere, wenn der Autor unter einem Pseudo-



Sonja Janisch: „Regelungen zur Frage, welche Inhalte eine Website aufweisen muss, finden sich in verschiedenen Gesetzen.“

nym aufgetreten ist. „Achten Sie auf eine klare Trennung zwischen eigenen und verlinkten Inhalten und entfernen Sie Links, sobald Ihnen eine Rechtsverletzung auf der verlinkten Website bekannt wird“, rät Janisch. „Löschen Sie rechtswidrige Inhalte aus Ihrem Online-Gästebuch oder Internet-Forum unverzüglich nach der ersten Abmahnung und überprüfen Sie sie regelmäßig nach erstmaliger Abmahnung auf ähnliche Rechtsverstöße und löschen Sie diese. Und: Provozieren Sie keine Rechtsverletzungen durch polarisierende Beiträge oder Ähnliches.“

Überwachung am Arbeitsplatz. „Eine Videoüberwachung am Arbeitsplatz ist ein technisches System zur Kontrolle der Arbeitnehmer, das die Menschenwürde berührt, auch wenn die Kontrolle nur ein Nebeneffekt ist“, stellte Mag. Wolfgang Goricnik von der Kammer für Arbeiter und Angestellte für Salzburg fest. Die Einrichtung eines solchen Systems bedarf – bei sonstiger Rechtswidrigkeit – nach § 96 Abs. 1 Z 3 Arbeitsverfassungsgesetz (ArbVG) der Zustimmung des Betriebsrates oder, wo ein solcher



Wolfgang Goricnik: „Videoüberwachung am Arbeitsplatz ist ein Kontrollsystem, das die Menschenwürde berührt.“

nicht besteht, nach § 10 Abs. 1 Arbeitsvertragsrechts-Anpassungsgesetz (AVRAG) der Zustimmung des Arbeitnehmers. Werden die Bilder digital aufgezeichnet, bedarf dies einer Vorabkontrolle durch die Datenschutzkommission nach § 18 Abs. 2 Z 1 Datenschutzgesetz, da die Bilder Rückschlüsse auf die rassische oder ethnische Herkunft, die religiöse Überzeugung (Turban, Kopftuch) oder die Gesundheit (Gesichtsfarbe, Gipsverbände) der aufgezeichneten Personen zulassen würden und besonders schutzwürdige Daten im Sinn des § 4 Abs. 2 DSGVO darstellen. Erst nach Prüfung durch die Datenschutzkommission darf der Betrieb einer solchen Datenanwendung aufgenommen werden.

Wenn die Nutzung des Internets durch den Arbeitgeber freigegeben wird, empfiehlt sich eine klare Regelung in Form einer Betriebsvereinbarung, welche Daten (Logfiles) abgespeichert werden dürfen. Aus den Logfiles kann immerhin ersehen werden, welche Websites sich jemand ansieht; die Einführung eines darauf abzielenden Kontrollsys-

tems würde wiederum die Menschenwürde berühren und bedürfte der Zustimmung des Betriebsrates oder des Arbeitnehmers. Ein System zur (sonstigen) automationsunterstützten Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten des Arbeitnehmers, die über die Ermittlung von allgemeinen Angaben zur Person und fachlichen Voraussetzungen hinausgehen, bedarf zwar nach § 96a ArbVG zu seiner Rechtswirksamkeit ebenfalls der Zustimmung des Betriebsrates, die aber durch Entscheidung der Schlichtungsstelle ersetzt werden kann.

Der Einsatz von „Spyware“ gegen Arbeitnehmer verletzt die Menschenwürde und ist daher immer rechtswidrig.

Was den E-Mail-Verkehr betrifft, ist zusätzlich nach § 93 Abs. 3 Telekommunikationsgesetz 2003 unzulässig das Mithören, Abhören, Aufzeichnen, Abfangen oder sonstige Überwachen von Nachrichten und der damit verbundenen Verkehrs- und Standortdaten sowie die Weitergabe von Informationen darüber durch andere Personen als einen Benutzer ohne Einwilligung aller beteiligten Benutzer. Dieses Kommunikationsgeheimnis gilt auch dann, wenn der Arbeitgeber kein Betreiber eines öffentlichen Kommunikationsnetzes ist. Da Regelungen zwar vorhanden sind, aber das Bewusstsein und die Rechtsdurchsetzung verbesserungsbedürftig erscheinen, wäre laut Goricnik die gesetzliche Einführung eines weisungsfrei gestellten und im Zusammenhang mit seiner fachlichen Tätigkeit dem Kündigungsschutz unterliegenden innerbetrieblichen Datenschutzbeauftragten sinnvoll.

Kurt Hickisch