Geschäftsstelle Dresden:
Königsbrücker Landstraße 40
01109 Dresden
Tel: 0351 8881251

Niederlassung Böblingen:
Otto-Lilienthal-Straße 36
71034 Böblingen
Tel: 07031 7145660

mail@sodalitas-gmbh.de
www.sodalitas-gmbh.de
Fax: 0351 8881252

IT-Ticker 03/2016

Der IT-Ticker 032016 informiert Sie über folgende Themen:

- Einschränkung der Linkfreiheit schützt Urheberrechtsinhaber
- Öffentliches WLAN: Keine Haftung des Anbieters, aber Passwortpflicht
- Sharehoster zu Schadensersatz verurteilt
- Bußgelder wegen Safe Harbor-Übermittlungen
- EU-US Privacy Shield in Kraft
- Schadensersatz bei Verstoß gegen Open Source Lizenz
- NIS-Richtlinie in Kraft getreten
- Auswirkung des Brexit im Bereich Datenschutzrecht

Einschränkung der Linkfreiheit schützt Urheberrechtsinhaber

In seinem Urteil vom 8. September 2016 hat der EuGH die Linkfreiheit für Unternehmen erheblich eingeschränkt. In seinem Urteil argumentiert der EuGH, dass von einer öffentlichen Wiedergabe ausgegangen werden könne, wenn Hyperlinks mit Gewinnerzielungsabsicht gesetzt würden. Von demjenigen, welcher mit Gewinnerzielungsabsicht Hyperlinks setze, könne erwartet werden, dass er die erforderlichen Prüfungen vornehmen würde, um sich zu vergewissern, dass das betroffene Werk auf der Webseite, zu welcher der Hyperlink führt, nicht unbefugt veröffentlicht wurde. Aus diesem Grunde sei zu vermuten, dass ein solches Setzen von Hyperlinks in voller Kenntnis der Geschütztheit des Werks und der etwaig fehlenden Erlaubnis des Urheberrechtsinhabers vorgenommen wurde.

Sofern diese widerlegliche Vermutung nicht entkräftet werden könne, stelle das Setzen des Hyperlinks eine öffentliche Wiedergabe dar und der Rechtsverletzer muss die entsprechenden Konsequenzen tragen, z.B. Schadensersatz. Die Vermutung kann zum Beispiel wiederlegt werden, wenn mangels eines „neuen Publikums“ keine öffentliche Wiedergabe gegeben ist. Dies ist der Fall, in dem die Werke, zu denen die Hyperlinks Zugang geben, auf einer anderen Webseite mit Erlaubnis des Rechtsinhabers frei zugänglich sind.

Somit ist zukünftig darauf zu achten, dass Urheberrechtsinhaber nicht nur gegen die ursprüngliche Veröffentlichung ihres Werks auf einer Webseite vorgehen können, sondern auch gegen jede Person, welche zu Erwerbszwecken einen Hyperlink zu einem unbefugt auf dieser Webseite veröffentlichten Werk setzt.

Praxistipp: Urheberrechtsinhaber haben mehr Möglichkeiten gegen die unrechtmäßige öffentliche Wiedergabe ihrer Werke vorzugehen. Dies bewirkt, dass ein Unternehmen, welches mit seiner Webseite Geld verdient beim Setzen eines Hyperlinks prüfen sollte, ob der Hyperlink zu unbefugt veröffentlichten Werken führt. Wie bislang darf durch das Setzen eines Hyperlinks keinesfalls eine Zugangsbeschränkung der Webseite umgangen werden.

Franziska Ladiges, Frankfurt/Main
f.ladiges@skwschwarz.de

Öffentliches WLAN:
Keine Haftung des Anbieters, aber Passwortpflicht

Die Frage war lange heiß diskutiert und wurde nun vom EuGH entschieden: Sind Anbieter offener WLAN-Netzwerke haftbar, wenn anonyme Nutzer darüber urheberrechtliche Verletzungen begehen? Das jüngste Urteil des EuGH (Urt. v. 15.09.2016 – Az. C-484/14) ist für gewerbliche Anbieter wie z.B. Hotels, Cafés, etc. Freud und Leid zugleich: Eine Haftung des Anbieters als „Störer" hat der Gerichtshof abgelehnt. Der Gewerbetreibende kann aber für die Zukunft verpflichtet werden, das WLAN-Netz mit angemessenen Vorkehrungen gegen weitere Verstöße absichern. Hierzu gehört insbesondere das Einrichten eines Passworts für das WLAN, welches an die Kunden erst nach Mitteilung des Namens herausgegeben werden darf. *Mehr dazu lesen ...*

Sven Preiss, LL.M., Berlin
s.preiss@skwschwarz.de

Sharehoster zu Schadensersatz verurteilt

Einer Pressemitteilung der GEMA zufolge hat diese vor dem LG München I einen urheberrechtlichen Schadensersatzanspruch gegen den Sharehoster „Uploaded" durchgesetzt (Urt. vom 10.08.2016, Az. 21 O 6197/14). Sharehoster wie „Uploaded" stellen Kunden Speicherplatz für das Hochladen von Dateien zur Verfügung. Das LG München I habe nun entschieden, dass Onlinedienste, deren Geschäftsmodelle auf der massenhaften Verletzung von Urheberrechten basieren, schadensersatzpflichtig sein können, weil diese Onlinedienste Links zu hochgeladenen Dateien generieren, die dann als öffentlich zugängliche Linksammlungen verbreitet werden. Das Landgericht München habe dies als einen Dienst angesehen, der eine spezifische Gefahrenquelle für Urheberrechtsverletzungen bilde. „Uploaded" sei demnach als „Gehilfe" der illegalen Zugänglichmachung von urheberrechtlich geschützten Inhalten in die Pflicht zu nehmen. Die Entscheidung ist noch nicht rechtskräftig.

Praxistipp: Verschuldensunabhängige Unterlassungsansprüche gegenüber Sharehostern waren in der Vergangenheit bereits Gegenstand gerichtlicher Entscheidungen. Falls die jüngste Münchener Entscheidung Schule macht und Gerichte künftig auch vom Verschulden ausgehen und Schadensersatz zusprechen, wird das Geschäftsmodell der Sharehoster rechtlich immer herausfordernder.

Daniel Pfeifer, München
d.pfeifer@skwschwarz.de

Bußgelder wegen Safe Harbor-Übermittlungen

In unserem IT-Ticker Q1/2016 hatten wir darüber berichtet, wie über die von der EU-Bereits im Oktober 2015 hat der EuGH in einer vielbeachteten Entscheidung, das Safe Harbor Abkommen für ungültig erklärt. Damit entfiel ein wesentlicher Pfeiler für eine rechtmäßige Datenübermittlung an US-Unternehmen. Unternehmen waren somit aufgefordert innerhalb einer mehrmonatige Umsetzungsfrist ihren US-amerikanischen Datentransfer auf einen anderen Pfeiler – insbesondere Standardvertragsklauseln – zu stützen.

Nach Ablauf dieser Umsetzungsfrist prüfte unter anderem der Hamburgische Datenschutzbeauftragte ab Februar 2016 die ordnungsgemäße Umstellung des Datentransfers in die USA. Im Zusammenhang mit dieser Prüfung wurden nun gegen drei Unternehmen bußgelder in Höhe von 8.000 Euro, 9.000

Euro und 11.000 Euro verhängt. Der Hamburger Datenschutzbeauftragte betont, dass die Bußgelder nur so gering ausgefallen sind, da die betroffenen Unternehmen im laufenden Bußgeldverfahren doch noch eine rechtmäßige Grundlage zur Datenübermittlung in die USA geschaffen haben. Unternehmen, welche ihren Datentransfer noch immer nicht auf die Standardvertragsklauseln umgestellt haben, müssen mit wesentlich höheren Bußgeldern rechnen – theoretisch sind Bußgelder bis zu einer Höhe von 300.000 Euro möglich.

Auch das Schicksal der Standardvertragsklauseln ist zu beachten. Denn die irische Datenschutzbehörde hat angekündigt, nun auch die Standardvertragsklauseln vor dem EuGH prüfen zu lassen.

Praxistipp: Unternehmen müssen die aktuellen Entwicklungen im Bereich des US-amerikanischen Datentransfers eng beobachten, um rechtzeitig notwendige Schritte zu ergreifen. Nur so können hohe Bußgelder vermieden werden.

Franziska Ladiges, Frankfurt/Main
f.ladiges@skwschwarz.de
Dr. Oliver Hornung, Frankfurt/Main
d.hornung@skwschwarz.de

EU-US Privacy Shield in Kraft

Am 8. Juli haben die EU-Mitgliedstaaten dem EU-US Privacy Shield mit mit großer Mehrheit zugestimmt. Die EU-Kommission ist an einigen Stellen auf die Forderungen der Datenschützer, allen voran der Artikel-29-Datenschutzgruppe, eingegangen und hat entsprechende Änderungen vorgenommen. Aufgrund dieser Änderungen hielt der Artikel-31-Ausschuss das abgeänderte EU-US Privacy Shield für zustimmungsfähig.

Die EU-Kommission hat am 12. Juli den Angemessenheits-Beschluss gefasst, mit welchem das EU-US Privacy Shield in Kraft getreten ist. Zu beachten ist, dass es sich bei diesem Beschluss um eine Adäquanzentscheidung handelt, welche nach dem Safe-Harbor-Urteil des EuGH durch die nationalen Datenschutzbehörden im Einzelfall auf die Konformität mit dem geltenden Datenschutzrecht geprüft werden kann.

Die Artikel-29-Datenschutzgruppe hat das EU-US Privacy Shield in einer ersten Stellungnahme akzeptiert, fordert allerdings, dass der vorgesehene jährliche Review des Abkommens genutzt wird, um das Abkommen weiter zu verbessern und bestehende Kritikpunkte auszuräumen.

Seit dem 1. Augst 2016 können sich nunmehr US-Unternehmen bei dem US-Department of Commerce unter dem neuen Schutzschild selbst zertifizieren. Diese Selbstzertifizierung ist im Rahmen einer jährlichen Re-Zertifizierung zu wiederholen. Die Privacy Shield-Liste beginnt sich langsam zu füllen. Größere US-Cloud-Provider sind mittlerweile auf der Liste zu finden.

Praxistipp: Die Kritik an EU-US Privacy Shield reißt nicht ab, sodass nicht auszuschließen ist, dass auch diese neue Angemessenheitsentscheidung der EU-Kommission vom EuGH überprüft und widrigenfalls gekippt wird. Aus Unternehmenssicht bleibt der internationale Datentransfer in die USA und andere unsichere Drittstaaten spannend und die weitere Rechtsentwicklung sollte aufmerksam beobachtet werden.

Franziska Ladiges, Frankfurt/Main
f.ladiges@skwschwarz.de
Dr. Oliver Hornung, Frankfurt/Main
d.hornung@skwschwarz.de
Nikolaus Bertermann, Berlin
n.bertermann@skwschwarz.de

Schadensersatz bei Verstoß gegen Open Source Lizenz

Erneut hat das Landgericht Bochum (LG Bochum, Urt. v. 03.03.2016 – Az. 8 O 294/15) eine Schadensersatzpflicht für die Nutzung einer Open Source Software unter Verstoß gegen die dafür geltende Open Source Lizenz bejaht.

Das Gericht geht davon aus, dass ein Verstoß des Empfängers der Software gegen die dafür geltende GNU General Public License Version 2 (GPL 2.0) zu einem Wegfall seiner Nutzungsrechte führt. Die Beklagte hatte die Software ohne den Lizenztext der GPL 2.0 verbreitet und deren Sourcecode weder mitgeliefert noch angeboten. Wegen dieser Verstöße gegen die GPL 2.0 sei die anschließende Nutzung unberechtigt. Dabei habe die Beklagte fahrlässig gehandelt, weshalb sie zum Schadensersatz verpflichtet sei. Das Landgericht geht für dessen Höhe wohl von der Vergütung für eine entsprechende kommerzielle Lizenz aus.

Das Urteil setzt die Rechtsprechung zur Schadensersatzpflicht bei Verstößen gegen eine Open Source Lizenz fort (siehe LG Bochum, Urt. v. 20.01.2011 – Az. 8 O 293/09; LG Köln, Urt. v. 17.07.2014 – Az. 14 O 463/13). Für Open Content unter einer Creative Commons Lizenz hatte das OLG Köln (Urt. v. 31.10.2014 – Az. 6 U 60/14; Anmerkung Schweinoch in NJW 2015, 794) eine Schadensersatzpflicht bei Lizenzverstößen verneint.

Praxistipp: Die Nichteinhaltung einer Open Source Lizenz kann nicht nur zum automatischen Wegfall der Nutzungsrechte führen, sondern zusätzlich auch zur Schadensersatzpflicht. Umso mehr Aufmerksamkeit sollte auf die Erfassung und dokumentierte Einhaltung von Open Source Lizenzen gerichtet werden.

Martin Schweinoch, München
m.schweinoch@skwschwarz.de

NIS-Richtlinie in Kraft getreten

Am 19.07.2016 ist die „Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union“ (kurz NIS-Richtlinie) im Amtsblatt der EU veröffentlicht worden. Die NIS-Richtlinie tritt damit am 08.08.2016 in Kraft.

Ziel der Richtlinie ist ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen innerhalb der EU. Zu diesem Zweck gibt sie Mindestanforderungen an die IT-Sicherheit vor und soll die Zusammenarbeit der EU-Mitgliedsstaaten auf dem Gebiet der Cybersicherheit stärken.

Diese haben bis zum 09.05.2018 Zeit, um die Vorgaben der NIS-Richtlinie in nationales Recht umzusetzen. Durch das 2015 in Kraft getretene IT-Sicherheitsgesetz dürfte der deutsche Gesetzgeber einen Großteil der EU-Mindestanforderungen an die IT-Sicherheit bereits vorab erfüllt haben. Einen Überblick über die Kerninhalte der NIS-Richtlinie und die Parallelen zum IT-Sicherheitsgesetz finden Sie auf unserer Webseite.

Daniel Meßmer, München
d.messmer@skwschwarz.de

Auswirkung des Brexit im Bereich Datenschutzrecht – Was kommt auf Unternehmen zu?

Der britische Wähler hat gesprochen und sich mit knapper Mehrheit für den Austritt des Vereinigten Königreichs aus dem „Projekt Europa“ entschieden. Gegenwärtig weiß niemand, ob, wann und wie der geplante Brexit stattfinden wird. Die bestehende politische aber auch rechtliche Unsicherheit bedeutet für Unternehmen eine große Herausforderung. Das betrifft auch den Bereich Datenschutzrecht. Hier wird entscheidend sein, ob es dem Vereinigten Königreich gelingt, nach dem Austritt aus der EU den Status eines sogenannten sicheren Drittstaates zu erlangen. In solche sicheren Drittstaaten dürfen Unternehmen der Europäischen Union personenbezogene Daten übermitteln, ohne zusätzliche Anforderungen erfüllen zu müssen. *Mehr dazu lesen ...*

Dr. Oliver Hornung, Frankfurt/Main
o.hornung@skwschwarz.de