Rundbrief Dezember 2016

Sehr geehrte Damen und Herren,

langsam aber sicher neigt sich das Jahr 2016 dem Ende entgegen! Im Anschluss an unseren Sonderrundbrief von August dieses Jahres erhalten Sie wie gewohnt unseren aktuellen Rundbrief mit wichtigen Entscheidungen aus der Rechtsprechung und praxisorientierten Fällen.

Wir wünschen Ihnen ein gesegnetes Weihnachtsfest und ein gesundes und erfolgreiches Jahr 2017!

Mit freundlichen Grüßen

Ihre SaphirIT GmbH

Störerhaftung bei Nutzung des voreingestellten WLAN-Passworts

Der Bundesgerichtshof (BGH) hatte kürzlich (erneut) einen Fall zu entscheiden, in dem die Frage zu klären war, ob Nutzer, die ein WLAN-Netzwerk betreiben und dieses über das im Router voreingestellte Passwort sichern, als sog. „Störer“ in Anspruch genommen werden können.

Der BGH hat dies – wie die Vorinstanzen auch – verneint. Im vorliegenden Fall war unstreitig, dass ein Actionfilm über den WLAN-Anschluss der Beklagten mehrfach öffentlich zugänglich gemacht worden war. Dies war durch einen unbekannten Dritten geschehen. Der Rechteinhaber nahm die Beklagte daher wegen des öffentlichen Zugänglichmachens dieses Filmwerks im Wege des sogenannten „File-sharings“ auf Ersatz von Abmahnkosten in Anspruch. Der Anschluss der Beklagten war über den als hinreichend sicher anerkannten Standard „WPA2“ und ein 16-stelliges Passwort gesichert. Dieses Passwort war im Router

SaphirIT GmbH
Sutthauser Straße 285
49080 Osnabrück
Geschäftsführer
Amtsgericht Osnabrück

www.saphirit.de
USt.-ID DE 268765300
Frank W. Stroot
HRB 203854

Datenschutz – IT-Sicherheit
Oldenburgische Landesbank AG
IBAN DE29 2802 0050 5042 8200 00
BIC OLBODEH2XXX

Telefon 0541/60079296
Telefax 0541/60079297
datenschutz@saphirit.de

der Beklagten bereits voreingestellt und wurde von der Beklagten nach Inbetriebnahme – im Gegensatz zu der Routerkennung (SSID) – nicht mehr verändert.

Der BGH hatte bereits mit dem Urteil „Sommer unseres Lebens“ (BGH, Urteil vom 12.05.2010, Az. I ZR 121/08) entschieden, dass für WLAN-Betreiber grundsätzlich eine Pflicht besteht, ausreichend lange und sichere Passwörter zu vergeben sowie eine Verschlüsselung nach aktuellem Standard einzusetzen. Diese Pflicht beinhaltet dabei auch, die Standardeinstellungen gegebenenfalls zu ändern. Fraglich war daher lediglich, ob diese Prüfpflichten auch die Änderung eines ursprünglich sicheren, voreingestellten Passwortes beinhalten.

Der BGH hat dies im aktuellen Fall verneint und festgestellt, dass die Beibehaltung eines vom Hersteller voreingestellten WLAN-Passwortes nur dann eine Verletzung von Prüfpflichten darstellen könne, wenn es sich nicht um ein für jedes Gerät individuell, sondern für eine Mehrzahl von Geräten verwendetes Passwort handele oder bereits bei der Inbetriebnahme Anhaltspunkte dafür bestanden, dass Dritte das voreingestellte Passwort entschlüsseln können. Solche Anhaltspunkte gab es nach Auffassung des Gerichts vorliegend nicht.

Ein Anspruch aus Störerhaftung wurde daher schließlich verneint.

SaphirIT-Tipp

Mit diesem Urteil hat der BGH die Prüfpflichten für WLAN-Betreiber weiter eingeschränkt. Echte Rechtssicherheit besteht auf diesem Gebiet jedoch noch nicht, so dass weiterhin Vorsicht geboten ist. Es kommt immer auf den Einzelfall an!

Holen Sie sich daher vor Inbetriebnahme eines WLAN-Netzwerkes unseren fachkundigen Rat ein!

Ausweiskopien ja oder nein

Die Frage, ob und in welchen Fällen Kopien des Personalausweises und anderer Ausweisdokumente angefertigt werden dürfen, hat die Gerichte und die Fachliteratur bereits des Öfteren beschäftigt.

Die Rechtsgrundlagen zur Beantwortung dieser Frage befinden sich weitgehend im Personalausweisgesetz (PAuswG) und dem Passgesetz (PassG). Ein generelles Kopierverbot besteht nach Auffassung des Bundesinnenministeriums nicht. Zum einen gebe es gesetzlich festgelegte Ausnahmen im Geldwäschegesetz (GwG) sowie im Telekommunikationsgesetz (TKG) und zum anderen gebe es anerkannte und an strenge Voraussetzungen geknüpfte Ausnahmen für die Anfertigung einer Ausweiskopie.

Folgende Grundsätze sollten unbedingt eingehalten werden, um rechtliche Risiken auszuschließen:

- Die Erstellung einer Kopie muss erforderlich sein. Dabei ist insbesondere zu prüfen, ob bereits die Vorlage des Personalausweises und ggf. die Anfertigung eines entsprechenden Vermerks (z. B.: „Personalausweis hat vorgelegen“) ausreichend sind. Die Erforderlichkeit entfällt, wenn der Personalausweis ohne großen Aufwand vor Ort vorgezeigt und eingesehen werden kann.

- Die Kopie darf ausschließlich zu Identifizierungszwecken verwendet werden. Eine weitergehende Nutzung ist rechtswidrig.

- Die Kopie muss als solche erkennbar sein (z.B. Aufdruck „Kopie“). Die Kopie darf nicht den Eindruck erwecken, dass es sich dabei selbst um ein Ausweisdokument handelt.

- Daten, die nicht zur Identifizierung benötigt werden, können und sollen von den Betroffenen auf der Kopie geschwärzt werden. Dies gilt insbesondere für die auf dem Ausweis aufgedruckte Zugangs- und Seriennummer. Die Betroffenen sind auf die Möglichkeit und Notwendigkeit der Schwärzung hinzuweisen. Die Angabe des Geburtsdatums und ggf. -ortes kann nur erforderlich sein, wenn trotz der vorgenannten Angaben eine Personenverwechslung möglich ist und das Unternehmen in seinem bisherigen Datenbestand überhaupt das Geburtsdatum oder den -ort als Referenzdatum gespeichert hat.

- Die Kopie ist vom Empfänger unverzüglich zu vernichten, sobald der mit der Kopie verfolgte Zweck erreicht ist. Eine Archivierung ist unzulässig. Sofern eine Protokollie-

rung erforderlich ist, genügt die Speicherung eines entsprechenden Vermerks „Ausweiskopie hat vorgelegen“.

- Eine automatisierte Speicherung der Ausweisdaten ist nach dem PAuswG unzulässig. Auch darf nach der Rechtsprechung der Personalausweis nicht gescannt und elektronisch gespeichert werden (Verwaltungsgericht Hannover, Urteil vom 28. November 2013, Az. 10 A 5342/11).

SaphirIT-Tipp

Nur wenn die oben genannten Vorgaben eingehalten werden, ist ein rechtssicherer Umgang mit Ausweisdokumenten bzw. mit deren Kopien möglich. Personenbezogene Daten sind stets mit besonderer Vertraulichkeit zu behandeln. Anderenfalls droht eine Inanspruchnahme durch die Betroffenen!

Sprechen Sie uns hierzu jederzeit gerne an!

Private Internetnutzung: Browserverlauf des Dienstrechners

Die Parteien stritten vor dem Landesarbeitsgericht Berlin-Brandenburg (Urteil vom 14.01.2016, Az. 5 Sa 657/15) über die Wirksamkeit einer außerordentlichen Kündigung durch den Arbeitgeber. Nach internen Hinweisen auf eine erhebliche private Nutzung des Internets durch den Arbeitnehmer wertete der Arbeitgeber den Browserverlauf ohne Einwilligung des Arbeitnehmers aus. Die Privatnutzung des Internets war nur in Ausnahmefällen während der Pausen erlaubt. Die Auswertung ergab, dass der Arbeitnehmer während der Arbeitszeit über einen Zeitraum von 30 Arbeitstagen im Umfang von knapp 40 Arbeitsstunden das Internet privat genutzt hatte. Nach Anhörung des Betriebsrats kündigte der Arbeitgeber fristlos.

Nach Ansicht des LAG Berlin-Brandenburg ist die Kündigung wirksam. Die unerlaubte Privatnutzung des Internets rechtfertige nach Abwägung der beiderseitigen Interessen eine sofortige Kündigung. Auch liege hinsichtlich des Browserverlaufs kein Beweisverwertungsverbot vor. Die Verwertung sei statthaft, da § 32 Bundesdatenschutzgesetz (BDSG) eine Speicherung und Auswertung des Browserverlaufs zur Missbrauchskontrolle auch ohne Einwilli-

gung des Betroffenen erlaube. Ebenfalls sei unerheblich, dass die Auswertung nicht in Anwesenheit des Betroffenen erfolgt ist. Das Ergebnis der Auswertung hätte sich nicht geändert.

Ferner ergebe sich ein Beweisverwertungsverbot auch nicht aus § 88 TKG. Das TKG findet vorliegend keine Anwendung, da der Arbeitgeber kein Diensteanbieter im Sinne des TKG sei.

SaphirIT-Tipp

Da bei der (teilweisen) Privatnutzung des Internets durch Arbeitnehmer noch immer Rechtsunsicherheiten bestehen, empfiehlt es sich aus Sicht des Arbeitgebers, die private Nutzung des Internets arbeitsvertraglich zu untersagen.

Problematisch ist jedoch, dass ein solch umfassendes Nutzungsverbot erfahrungsgemäß praktisch nur schwer umsetzbar ist. Es ist daher ebenfalls ratsam, im Falle der Gestattung von Privatnutzung deren Umfang sowie die arbeitgeberseitigen Zugriffs- und Prüfungsrechte detailliert zu regeln.

Datenschutzerklärung bei Online-Kontaktformular

Das Landgericht Berlin hat einen Fall entschieden, in dem es um die Frage ging, welche Auswirkungen es hat, wenn ein Online-Kontaktformular ohne datenschutzrechtliche Aufklärung verwendet wird. Die Antragsgegnerin hat dabei ein Kontaktformular verwendet, in das der Nutzer im Falle der Kommunikationsaufnahme personenbezogene Daten wie Name und E-Mail-Adresse eintragen muss. Dabei werden auf der Homepage keine Angaben zu Art, Umfang und Zweck der Erhebung und Verwendung der personenbezogenen Daten gemacht.

Der Antragsteller war der Ansicht, dass die Antragsgegnerin gemäß § 13 Telemediengesetz (TMG) darüber aufzuklären habe. Die Vorschrift sei darüber hinaus eine das Marktverhalten regelnde Norm. Der Antragsteller hat die Antragsgegnerin abgemahnt und zur Abgabe einer strafbewehrten Unterlassungserklärung aufgefordert. Die Antragsgegnerin war der Auffassung, dass ein wettbewerbsrechtlicher Verstoß gegen das BDSG nicht vorliege.

Das Gericht hat der Antragsgegnerin im Wege einer einstweiligen Verfügung zunächst untersagt, im Internet zu Zwecken des Wettbewerbs Dienstleistungen eines Immobilienmaklers zu bewerben und bzw. oder bewerben zu lassen, ohne gleichzeitig die gemäß § 13 TMG notwendigen Informationen zur Verfügung zu stellen bzw. stellen zu lassen. Dagegen hat die Antragsgegnerin Widerspruch erhoben.

Das Gericht hat die einstweilige Verfügung daraufhin aufgehoben und festgestellt, dass dem Antragsteller der geltend gemachte Unterlassungsanspruch gemäß § 3a des Gesetzes gegen den unlauteren Wettbewerb (UWG) in Verbindung mit § 13 TMG nicht zusteht.

Gemäß § 13 TMG hat jeder Diensteanbieter den Nutzer vor Beginn des Nutzungsvorgangs über Art, Nutzung und Zweck der Erhebung und Verwendung personenbezogener Daten aufzuklären. Unstreitig ist eine solche Aufklärung vorliegend zu keinem Zeitpunkt erfolgt. Ein Verstoß gegen das UWG lässt sich nach Auffassung des Gerichts allerdings nicht ohne weiteres ableiten. Die Nichtaufklärung habe keine spürbare Auswirkung auf die Mitbewerber der Antragsgegnerin. Es habe sich nicht um eine Datenerhebung zum Zwecke der Werbung gehandelt, sondern lediglich um die Angabe des Namens und einer E-Mail-Anschrift, welche allein dazu gedient habe, mit der Antragsgegnerin Kontakt aufzunehmen. Dies sei ebenso per Telefon oder durch eine vom Interessenten selbst abgeschickte E-Mail möglich gewesen. Dass die Daten des Nutzers bei der Nutzung eines Kontaktformulars direkt auf der Homepage gespeichert würden, habe nur Auswirkungen auf den Nutzer. Der Wettbewerb selbst sei dadurch jedoch nicht tangiert.

SaphirIT-Meinung

Eine unserer Ansicht nach überzeugende Begründung des Landgerichts Berlin, die für Klarheit sorgt. Es wurde klargestellt, dass nicht jeder Verstoß gegen § 13 TMG unmittelbare Auswirkungen auf die Regelungen des Wettbewerbsrechts hat.

Der „Brexit“ und seine Folgen

Ein zentrales Thema dieses Jahres – auch aus datenschutzrechtlicher Sicht – war der sogenannte „Brexit“. Mehr als fünfzig Prozent der Wähler des Vereinigten Königreichs von Großbritannien und Nordirland stimmten für einen Austritt aus der Europäischen Union. Es ist wei-

terhin davon auszugehen, dass dieser Austritt auch tatsächlich erfolgen wird. Es sind weitreichende gesellschaftliche, wirtschaftliche und rechtliche Auswirkungen zu erwarten.

Noch ist es allerdings nicht soweit. Das Vereinigte Königreich bleibt vorerst ein vollwertiges Mitglied der EU. Ein Austritt aus der EU erfordert zunächst einen entsprechenden Antrag nach Art. 50 des EU-Vertrages. Ein solcher Antrag ist bislang nicht erfolgt. Nach Auskunft der britischen Premierministerin Theresa May soll der Antrag formell im ersten Quartal 2017 gestellt werden.

Daher bleibt datenschutzrechtlich zunächst alles unverändert. Erst wenn der Austritt formell vollzogen ist, ist entscheidend, ob das Vereinigte Königreich als Land mit einem angemessenen Datenschutzniveau gilt. Dies wird von den zukünftigen britischen Regelungen zum Datenschutz abhängen. Derzeit ist jedoch davon auszugehen, dass ein ausreichendes Datenschutzniveau erhalten bleibt. Dies allein schon vor dem Hintergrund, dass die Wettbewerbsfähigkeit des Vereinigten Königreichs sichergestellt werden soll.

SaphirIT-Tipp

Es ist daher ratsam, für die Zeit zwischen vollzogenem Austritt und der zu erwartenden Neuvergabe des Status als Staat mit angemessenem Datenschutzniveau das erforderliche Datenschutzniveau einzelvertraglich, beispielsweise unter Verwendung der EU-Standardvertragsklauseln, herzustellen.

Sofern der Austritt tatsächlich erfolgt, ist davon auszugehen, dass eine kurzfristige Lösung aus datenschutzrechtlicher Sicht gefunden werden kann. Jedenfalls sind durch den bevorstehenden „Brexit“ derzeit viele offene Fragen zu klären!

Sprechen Sie uns hierzu jederzeit gerne an!