HEUSSEN
Rechtsanwaltsgesellschaft mbH

NEWSLETTER DATENSCHUTZ 06/2016

AKTUELLES 1

1. Facebook: Beiträge können nachträglich geändert werden 1

2. Keine Cookies Dritter bei Google 1

3. Besonders viele Anfragen aus Deutschland 2

4. Ermittlungen gegen Skype 2

5. Ungeschützte Verbindungsdaten in den USA 3

BEITRAG 3

AUS DER RECHTSPRECHUNG 6

1. Videoüberwachung in einer Wohnungseigentümergemeinschaft 6

2. Telekom: IP-Adressen dürfen eine Woche lang gespeichert werden 7

München, im Juni 2016

AKTUELLES

1. Facebook: Beiträge können nachträglich geändert werden

Für viele Facebook-Nutzer ist es eine freudige Nachricht: Bald soll es nach eigenen Aussagen des Unternehmens möglich sein, Beiträge auch nachträglich zu verändern. Bisher konnten Beiträge nur ganz gelöscht werden, eine Änderung war nicht möglich.

In Deutschland ist die Funktion noch nicht flächendeckend verfügbar, soll den Nutzern aber nach und nach zur Verfügung gestellt werden. Auch für Smartphones soll die Android-App aktualisiert und um die neue Funktion erweitert werden. Im rechten Pulldown-Menü des Posts soll in Zukunft die Möglichkeit „Beitrag bearbeiten“ eingefügt werden.

Facebook war bisher bei der Einführung eher zögerlich, was vor allem mit der Befürchtung zu tun hat, es könnte Missbrauch mit der neuen Funktion getrieben werden. So könnten Nutzer mit einem harmlosen Post wie zum Beispiel „Ich liebe Eis!“ viele Likes von anderen Nutzern sammeln – und dann später den Text des Posts in etwas Anstößiges oder einen Werbetext ändern. Die Likes würden so in einem ganz anderen, nicht gewollten Kontext erscheinen. Um dies zu verhindern führt Facebook gleichzeitig einen Bearbeitungsverlauf ein. Mit dessen Hilfe kann nachvollzogen werden, ob tatsächlich nur Rechtschreibfehler ausgebügelt wurden oder der ganze Sinn des Posts verändert wurde.

2. Keine Cookies Dritter bei Google

Cookies von Drittanbietern, sogenannte Third-Party-Cookies, soll es in Zukunft bei Google nicht mehr geben. Das Unternehmen möchte den neuen Standard AdID durchsetzen, der nach eigenen Aussagen den Nutzern mehr Privatsphäre bringen soll.

Third Party Cookies – so werden Cookies bezeichnet, die nicht von der Website selbst platziert werden, sondern Inhalte Dritter darstellen. Klassische Beispiele bilden die von Dritten gelieferte Werbung und sogenannte „Social Widgets“ wie Facebooks Like-Button.

Google möchte diese Cookies nun nicht mehr nutzen und nach eigenen Angaben mit einer neu entwickelten Technologie namens AdID ersetzen. Diese Technologie soll anonymes Datensammeln werbetreibender Unternehmen ermöglichen. Google möchte die Funktion Unternehmen und Werbenetzwerken künftig zur Verfügung stellen.

In den kommenden Monaten möchte das Unternehmen mit Regierungsstellen und Verbraucherorganisationen verhandeln. Das Unternehmen selbst bezeichnet seinen neuen Standard als Verbesserung für die Privatsphäre des Nutzers, Details sind aber noch geheim. Herumgesprochen hat sich jedoch bisher, dass es Nutzern ermöglicht werden soll, in einen privaten Modus umzuschalten und so zu verhindern, dass Informationen gesammelt werden können.

Dies soll Nutzer vor dem sogenannten Tracking schützen, welches mittels Cookies von Drittanbietern möglich ist.

3. Besonders viele Anfragen aus Deutschland

Nicht nur amerikanische Behörden sammeln gern Daten – auch auf deutsche Behörden trifft dies offenbar zu. So erklärte Microsoft kürzlich, dass Deutschland zu den Ländern gehöre, die die meisten Anfragen zu Nutzerdaten an das Unternehmen richten.

Im ersten Halbjahr 2013 brachten es deutsche Behörden so immerhin auf 6.000 Anfragen hinsichtlich der Herausgabe von Nutzerdaten. Aus einem jüngst veröffentlichten Transparenzbericht von Microsoft geht hervor, dass Deutschland damit nach den USA und der Türkei das Land mit den meisten Nachfragen darstellt.

Nach eigenen Angaben gibt der Konzern jedoch im Rahmen normaler Ermittlungserfahren keine Daten an deutsche Behörden heraus. Anders sei dies nur bei lebensgefährlichen Notfällen wie Selbstmordversuchen oder Entführungen. Dies habe auch nur 37 der 6.000 Anfragen betroffen. Microsoft gibt weiterhin an, dass nur eine äußerst geringe Zahl von Nutzern überhaupt von Anfragen betroffen ist, eigenen Angaben zufolge nur etwa jeder Zehntausendste.

4. Ermittlungen gegen Skype

Ärger für den Internetdienst Skype: Luxemburgs Datenschutzkommission hat Ermittlungen gegen das Unternehmen aufgenommen. Anlass war eine mögliche Datenweitergabe an den amerikanischen Geheimdienst NSA.

Die Untersuchung soll klären, ob Skype durch die Weitergabe von Daten im Rahmen des Spähprogramms Prism gegen Luxemburger Gesetze verstoßen hat. Die Verfassung des Landes umfasst auch den Schutz der Privatsphäre, jedoch ist eine Überwachung der Telekommunikation durch richterlichen Beschluss oder die Anordnung durch politische Organe möglich. Zur Aufklärung wurden nach Angaben des Präsidenten der Luxemburger Datenschutzkommission Gérard Lommel Fragebögen an das Unternehmen Skype geschickt und umfangreiche Untersuchungen aufgenommen.

Erst wenn ein Verstoß des Unternehmens gegen geltendes Recht festgestellt werden kann, soll entschieden werden, ob ein Verfahren gegen das Unternehmen eröffnet wird.

5. Ungeschützte Verbindungsdaten in den USA

Verbindungsdaten zu Telefongesprächen werden in den USA nicht als Teil der Privatsphäre angesehen. Dies ergab die Auswertung eines Dokuments des US-Geheimgerichts Fisc. Konsequenz ist, dass die Verbindungsdaten ohne richterliche Anordnung an Behörden weitergegeben werden dürfen.

Das Gericht begründet seine Ansicht damit, dass Verbindungsdaten nicht schutzwürdig seien. Es verweist dabei auf Präzedenzfälle in der Rechtsprechung. Nach Ansicht des Gerichts würden die Verbindungsdaten ohnehin von Telefongesellschaften zentral gespeichert, zum Beispiel um die Rechnungsstellung zu ermöglichen. Bürger müssten daher damit rechnen, dass Behörden Zugriff auf die Daten haben könnten. In der Folge können diese Daten ohne weitere Hürden wie eine richterliche Anordnung an Behörden herausgegeben werden, sie werden nicht vom Recht auf Privatsphäre geschützt.

Diese Regelung in den USA geht damit weit über die bis 2010 geltenden Regelungen in Deutschland zur Vorratsdatenspeicherung hinaus. Nach deutschem Recht waren Abfragen nur in Einzelfällen und nur mit richterlicher Anordnung möglich. Praktisch können Behörden in den USA sich eine 90 Tage gültige Generalvollmacht in einem nichtöffentlichen Verfahren besorgen. Mit dieser Vollmacht ist ein Zugriff auf alle Verbindungsdaten möglich und sie kann jederzeit erneuert werden.

BEITRAG

EU Parlament: Alles Wichtige rund um den Beschluss der neuen Verordnung zum Datenschutz

Am Montag den 21. Oktober 2013 hat sich das EU-Parlament auf neue Vorschriften zum Thema Datenschutz geeinigt. Diese sollen die bisherige Datenschutz-Richtlinie ablösen, die nunmehr seit 18 Jahren in Kraft ist und schon lang nicht mehr als zeitgemäß gilt. Rund eineinhalb Jahre rangen die EU-Politiker um den Inhalt der neuen Richtlinie, die den Datenschutz in den 28 Mitgliedsstaaten erstmalig vereinheitlichen soll. Bearbeitet wurde der Entwurf der EU-Justizkommissarin Viviane Reding von Jan Philipp-Albrecht, einem jungen Grünen-Politiker.

Bedeutung der geplanten Richtlinie

Das neue Gesetz ist immens wichtig, da es über den Datenschutz und die Privatsphäre von jedem EU-Bürger und damit mehr als 500 Millionen Menschen entscheiden soll.

Allein die jüngsten Enthüllungen über die Späh-Skandale rund um Edward Snowden haben mehr als deutlich gemacht, was für ein brandaktuelles und wichtiges Thema der Datenschutz ist. Nach Angaben der Sueddeutschen Zeitung liest die NSA allein in Deutschland jeden Monat bis zu 500 Millionen Kommunikationsverbindungen mit.

Auch für US-Unternehmen im Allgemeinen war es bisher recht einfach, den strengen Datenschutz einiger europäischer Länder zu umgehen, indem sie sich in den Mitgliedsstaaten ansiedelten, in denen die lockersten Datenschutzbestimmungen gelten. So agiert zum Beispiel Facebook von Irland aus.

Dies soll nach Inkrafttreten der neuen Richtlinie nicht mehr möglich sein. Dann würde nur noch ein einheitlicher Datenschutzstandard in ganz Europa gelten.

Wie brisant das Thema ist, zeigt auch allein die große Zahl der Änderungsantrage, auf denen der jetzige Entwurf basiert: Rund 3999 Anträge reichten die Abgeordneten ein.

Was regelt der Entwurf?

Der Verordnung liegen mehrere Faustregeln zu Grunde: Zunächst wird das Recht auf Datenschutz auf die Ebene eines europäischen Grundrechts erhoben. Als Grundrecht ist dieses in Deutschland schon seit 1983 anerkannt. Grundsätzlich sollen nach der Verordnung nur so viele Daten gesammelt werden dürfen, wie es tatsächlich nötig ist – ein Prinzip, das auch dem deutschen Datenschutzrecht innewohnt. Darüber hinaus soll jeder Person das Recht zustehen, die Löschung seiner eigenen personenbezogenen Daten zu verlangen.

Ein lang diskutiertes Anliegen hat es jedoch nicht in den Entwurf geschafft – das sogenannte „Recht auf Vergessen“. Dieses hätte weiter gereicht als das bloße Recht auf Löschung, galt aber vielfach als in der Praxis kaum umsetzbar. Besonders Internetfirmen kritisierten, dass Daten leicht kopiert werden könnten und sich diese Kopien nicht bis in den letzten Winkel des Internets zurückverfolgen ließen.

Datenschutzverstöße sollen im neuen Entwurf härter geahndet werden können als bisher, bis zu 5 Prozent des Jahresumsatzes eines Unternehmens können als Strafe festgesetzt werden.

Für Unternehmen, die in einem Jahr die Daten von mehr als 5.000 Betroffenen verarbeiten, besteht nach dem Entwurf eine Pflicht zur Bestellung eines Datenschutzbeauftragten.

Auch der Skandal rund um Edward Snowden hat seine Spuren in der neuen Verordnung hinterlassen: Ein auf Drängen der US-Regierung eigentlich schon gestrichener Passus wurde erneut in die Verordnung aufgenommen. Danach dürfen Unternehmen, die durch Sicherheitsbehörden von Nicht-EU-Ländern dazu aufgefordert werden, Daten über EU-Bürger herauszugeben, diese Daten nur weitergeben, wenn zwischen der EU und dem Drittstaat ein einschlägiges Abkommen besteht (sogenannte FISA-Klausel). Ein solches Abkommen kann zum Beispiel in der Form von Verträgen, Rechtshilfeabkommen oder EU-Verordnungen bestehen. Zusätzlich soll jeder Einzelfall von der für das Unternehmen zuständigen Datenschutzbehörde genehmigt werden müssen.

Bewertung des Entwurfs durch Experten

Der Berichterstatter der Grünen, Jan Philipp Albrecht, sieht die Abstimmung über den Entwurf als „Meilenstein auf dem Weg zu einem starken EU-Datenschutz“. Auch die anderen Parteien sehen den Entwurf größtenteils positiv.

Von Datenschützern wurde jedoch bislang kritisiert, dass der Entwurf zu viele ungenaue Formulierungen enthalte. Als Beispiel wird angeführt, dass Daten bei „berechtigtem Interesse“ auch ohne Zustimmung des Nutzers verarbeitet werden könnten. Was unter diesem berechtigten Interesse zu verstehen sei, könne sehr weit ausgelegt werden und sei nicht hinreichend klar.

Bundesinnenminister Hans-Peter Friedrich (CSU) sieht noch viel Änderungsbedarf am Entwurf. Gegenüber der Zeitung „Die Welt“ äußerte er sich kritisch: „Es ist noch viel handwerkliche Arbeit nötig, um die Verordnung so auszugestalten, dass sie die hohen deutschen Datenschutzstandards widerspiegelt, praxistauglich ist und zugleich auf die Herausforderungen des Internetzeitalters vernünftige Antworten gibt.“

Die nächsten Schritte

Als nächster Schritt geht der Entwurf in den sogenannten „Trilog“. Die EU-Kommission und der EU-Ministerrat werden mit dem EU-Parlament über den Entwurf verhandeln. Auf Druck der Lobby könnte der Entwurf daher auch noch abgeschwächt werden.

Jan Philipp Albrecht hofft, dass die Verordnung noch vor der Europawahl im Mai 2014 in Kraft treten wird.

AUS DER RECHTSPRECHUNG

1. Videoüberwachung in einer Wohnungseigentümergemeinschaft

In einem aktuellen Beschluss vom 24. Mai 2013 hat der BGH entschieden, dass Wohnungseigentümergemeinschaften dann Videoüberwachungsanlagen installieren dürfen, wenn sie sich an die Vorgaben des BDSG halten und damit die Privatsphäre der Mieter achten. Insbesondere müssen dafür Regeln hinsichtlich des Umfangs und die Bedingungen der Überwachung festgelegt werden.

Eine Wohnungseigentümergesellschaft hatte als Reaktion auf einem Farbanschlag im Eingangsbereich eine Videoüberwachungsanlage installiert. Was zunächst als temporäre Lösung geplant war, sollte später dann aufgrund eines Beschlusses der Wohnungseigentümergesellschaft fortgesetzt werden. Als Grund wurde angegeben, dass ein Überblick hinsichtlich von Prostitution und bordellartigen Betrieben geschaffen werden soll. Eine Wohnungseigentümerin wandte sich jedoch hiergegen und forderte den Abbau der Anlage. Ihr Antrag wurde von der Versammlung abgelehnt. Gegen diese Ablehnung erhob die Eigentümerin Klage.

Der BGH entschied hierzu, dass der Betrieb einer Überwachungsanlage grundsätzlich zulässig sei, solange die Überwachung durch die Gesellschaft erfolgt und die Voraussetzungen des § 6b BDSG eingehalten werden. Als zusätzliche Voraussetzung forderte der BGH, dass bei einer Interessenabwägung das Interesse der Wohnungseigentumsgesellschaft an der Überwachung das Interesse von möglicherweise betroffenen Dritten am Schutz ihrer Privatsphäre überwiegt. Als Beispiel für ein Überwiegen führte der BGH an, dass mit der Überwachung Straftaten gegen das Gemeinschaftseigentum verhindert werden sollen. Die Regeln für den Betrieb der Überwachung müssen dabei aber von der Wohnungseigentümergesellschaft verbindlich festgelegt werden, was Transparenz gegenüber Dritten garantieren soll. Angrenzende öffentliche Flächen oder andere Grundstücke dürfen von der Überwachung nicht mit betroffen werden. Zudem darf die Überwachung nur in einem verhältnismäßigen Rahmen vorgenommen werden.

Im Fall gab der BGH der Klägerin Recht und bestätige, dass ihr Anspruch auf Abschaltung der Anlage bestand. Zum einen bestand laut des Gerichts der ursprüngliche Zweck der Verhinderung von Straftaten nicht mehr fort, es sei zu einer schleichenden Ausbreitung der Überwachung gekommen. Zum anderen seien Umfang und Zweck der Überwachung nicht ordnungsgemäß von der Wohnungseigentümergesellschaft festgelegt worden. Demnach lagen die Voraussetzungen für das Weiterbetreiben der Überwachungsanlage nicht vor.

2. Telekom: IP-Adressen dürfen eine Woche lang gespeichert werden

IP-Adressen dürfen von Providern anlasslos bis zu eine Woche lang gespeichert werden – das entschied das OLG Frankfurt am 28. August 2013 (13 U 105/07).

Geklagt hatte ein Kunde der Telekom, der forderte, dass der Provider seine IP-Adressen sofort löschen müsse. Dem gegenüber wandte das beklagte Unternehmen ein, dass die Daten für Abrechnungszwecke und zur Aufrechterhaltung des Betriebs für einige Tage gespeichert werden müssten.

Der Kläger war in der Vergangenheit bereits zweimal vor den deutschen Gerichten gescheitert: Sowohl das Landgericht Darmstadt als auch das OLG Frankfurt hatten seinem Begehren nicht stattgegeben. Danach wandte er sich erfolgreich an den BGH, mit dem Ergebnis, dass der Rechtsstreit zur erneuten Verhandlung an das OLG Frankfurt zurückgegeben werden musste. Grund dafür war nach Ansicht der Karlsruher Richter, dass die Richter in Frankfurt den Angaben der Telekom zu leicht Glauben geschenkt hätten. Es müsse genau überprüft werden, ob eine Speicherung für eine Woche wirklich nötig sei.

Doch auch nachdem das OLG Frankfurt ein Sachverständigengutachten zu dieser Frage eingeholt hatte, blieb es bei seiner Position und wies die Klage ab: Das Gutachten des Sachverständigen und auch ein von der Telekom gleichzeitig in Auftrag gegebenes Gutachten bestätigten unabhängig voneinander, dass eine Speicherung von einer Woche nötig sei. Eine Speicherung über einen Zeitraum von einer Woche sei dann nötig, wenn die Daten zur Beseitigung von Gefahrenabwehr wie zum Beispiel beim Spam-Versand nötig seien.

Der Kläger hat jedoch bereits angekündigt, gegen die Entscheidung erneut Rechtsmittel einlegen zu wollen.

Über diesen Newsletter

Die Autoren dieser Ausgabe sind in der Praxisgruppe IT-, IP- und Medienrecht tätig.

Mit unserem Newsletter möchten wir unsere Mandanten und interessierte Dritte über aktuelle Entwicklungen in Gesetzgebung, Rechtsprechung und Literatur informieren. Sollten Sie an diesen Informationen nicht interessiert sein, bitten wir Sie, uns dies per E-Mail mitzuteilen.

Sofern Sie zu bestimmten Themen oder zum Newsletter insgesamt Fragen oder Anregungen haben, können Sie sich jederzeit gerne an die Ihnen bekannten Ansprechpartner wenden. Gerne greifen wir auch Ihre Ideen für künftige Beiträge oder weitere Empfänger des Newsletters auf. Bitte wenden Sie sich an: georg.schroeder@heussen-law.de.

Ihre Ansprechpartner:

Dr. Georg F. Schröder, LL.M.
Rechtsanwalt

Fachbereich: IT-Recht, Luftverkehrsrecht
Schwerpunkt: EDV–Recht, IT-Security, Recht des Internet, Informationstechnologie, Electronic Commerce, Cyberlaw, Luftverkehrsrecht

georg.schroeder@heussen-law.de

www.heussen-law.de
www.heussen-datenschutz.de

Verantwortlich i.S.d. MDStV und des Presserechts:
RA Dr. Georg F. Schröder

Herausgeber
Heussen Rechtsanwaltsgesellschaft mbH
Amtsgericht München, HRB: 200015
Geschäftsführung: RA Christoph Hamm

Haftungsausschluss
Dieser Newsletter stellt ausgewählte Themen im Überblick dar und ersetzt nicht die rechtliche Beratung im Einzelfall. Wir bitten um Ihr Verständnis dafür, dass wir für die Richtigkeit und Vollständigkeit der in diesem Newsletter enthaltenen Angaben trotz sorgfältiger Recherche keine Haftung übernehmen.