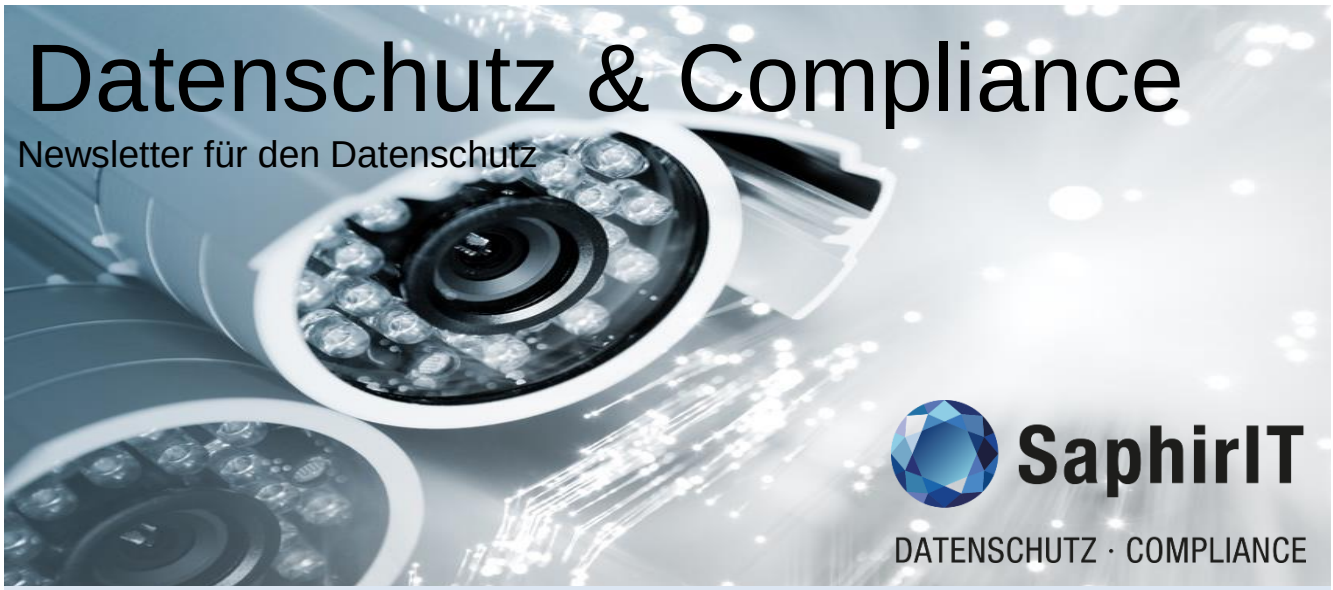

Ausgabe Juli 2017 | Seite 17-23

INHALT

Sehr geehrte Damen und Herren,

hiermit übersenden wir Ihnen unseren aktuellen Newsletter Juli 2017.

Wir wünschen Ihnen viel Spaß bei der Lektüre.

Mit freundlichen Grüßen
Ihre SaphirIT GmbH

Bundestag beschließt Netzwerkdurchsetzungsgesetz (NetzDG)

- Freie Meinungsäußerung in Gefahr? -

Der Bundestag hat am 30. Juni für den umstrittenen Gesetzentwurf von Bundesjustizminister Heiko Maas zur Bekämpfung von Fake News und Hate Speech im Internet gestimmt.

Das Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken schreibt Netzbetreibern wie Facebook, Twitter und YouTube vor, offensichtlich rechtswidrige Inhalte binnen 24 Stunden nach einem entsprechenden Hinweis zu löschen. Für komplexe oder nicht eindeutige Fälle wird den Verantwortlichen eine Frist von sieben Tagen gewährt.

Bei systematischen Verstößen drohen Bußgelder von bis zu 50 Millionen Euro.

Bereits jetzt wird kritisiert, dass mit dem Gesetz allein den Unternehmen die Entscheidung

darüber überlassen wird, was rechtmäßig ist und was nicht. Ferner würden Betreiber angesichts der hohen Bußgeldgefahr im Zweifel immer eher löschen. Es bestünde die Gefahr von *Overblocking*.

Es würden demnach tendenziell sehr viele und unter Umständen auch rechtmäßige Beiträge gelöscht.

Als besonders problematisch stellt sich die Gefahr einer Einschränkung der Meinungsfreiheit dar. Unternehmen könnten sich aus Angst vor den Bußgeldern in Grenzfällen eher für eine Löschung entscheiden.

Da viele betroffene Unternehmen ihren Sitz im Ausland haben sieht das Gesetz weiter vor, dass diese einen „Zustellungsbevollmächtigten“ in Deutschland haben müssen, der auf Beschwerden reagieren soll.

Neben dem Problem einer Vereinbarkeit mit dem Grundgesetz bestehen fernen auch Zweifel, ob das neue Gesetz mit europäischem Recht vereinbar ist. Ob das Gesetz vom Europäischen Gerichtshof nach dem Gesetz der Vorratsdatenspeicherung auch gekippt wird, wird man sehen. Wir werden weiter berichten.

Abmahngefahr bei WhatsApp?

- Nutzer müssen Einwilligung aller ihrer Kontakte einholen -

Das Amtsgericht Bad Hersfeld hat mit Beschluss vom 15.05.2017 entschieden, dass Eltern dazu verpflichtet sind, die Smartphone Nutzung ihrer Kinder zu begleiten und zu beaufsichtigen.

Nutzt das Kind WhatsApp treffe die Eltern die Pflicht ihr Kind im Hinblick auf Gefahren des Messenger Dienstes aufzuklären und die erforderlichen Schutzmaßnahmen zu treffen.

Wer die Weitergabe von Daten (z.B. Handynummern) seiner Kontaktpersonen zulässt, ohne von diesen vorher jeweils die Erlaubnis eingeholt zu haben, begehe gegenüber dieser Person eine deliktische Handlung und begebe sich in die Gefahr von den betroffenen Personen/Kontakten kostenpflichtig abgemahnt zu werden.

Die Eltern seien im entschiedenen Fall dazu verpflichtet gewesen, von allen Personen, welche sich im Adressbuch des Kindes befinden eine schriftliche Einverständniserklärung dahingehend einzuholen, „ob diese Personen damit einverstanden sind, dass das Kind in dem Adressbuch seines Smartphones die Telefonnummer(n) und den Namen – wenn ja, in welcher Form (Pseudonym, Kürzel oder aber Vor- oder/und Nachname als Klardatum) – der jeweiligen Person speichert und dass die Daten von dort dann regelmäßig über die von dem Kind gleichzeitig genutzte Applikation „WhatsApp“ an den Betreiber WhatsApp Inc. in Kalifornien/USA übertragen / hochgeladen werden, wo diese Daten zu vielfältigen Zwe-

cken des Betreibers laut dessen Nutzungsbedingungen frei weiter verwendet werden können.“

Die Nutzung von WhatsApp stelle für das Vermögen des Kindes eine Gefahr dar. Es bestehe nämlich „bei nicht weiter rechtlich abgesicherter Nutzung der App die konkrete Gefahr, dass das Kind wegen eines i.S.v. § 823 BGB deliktischen rechtswidrigen Verhaltens durch andere Personen abgemahnt und gemäß § 1004 BGB analog zur Unterlassung aufgefordert würde.“

Solche Abmahnungen sind, insbesondere wenn hierfür noch eingeschaltete Rechtsanwälte tätig werden, typischerweise mit intensiven Kosten verbunden, welche bei anwaltlicher Betätigung regelmäßig im dreistelligen Bereich zu verorten sind.

Ein deliktisches Verhalten des Kindes sei somit darin zu sehen, dass Nutzer von WhatsApp dauerhaft Daten über andere Nutzer an WhatsApp weiterleiten, ohne dazu überhaupt befugt zu sein.

Welche Auswirkungen genau dieser Beschluss nach sich zieht, wird man sehen. Es kann allerdings nach momentanem Stand davon ausgegangen werden, dass WhatsApp Nutzern im allgemeinen keine Abmahnwelle droht, auch wenn das Amtsgericht Bad Hersfeld dies im konkreten Fall so entschied.

Was der Beschluss erstmal verursacht hat, ist eine große Verunsicherung bei weniger rechtskundigen Personen.

Zunächst kann man feststellen, dass die Ausführungen des AG Bad Hersfeld zu der Weitergabe einzelner Kontaktdaten an den Betreiber wohl richtig sind. Zumindest bei der erstmaligen Nutzung von WhatsApp werden Kontaktdaten ausgelesen, um festzustellen, ob bekannte Nutzer WhatsApp bereits nutzen.

Entscheidend ist jetzt allerdings, ob jeder private Nutzer der App, für die tatsächliche Verarbeitung des Anbieters verantwortlich ist und ob betroffene Kontakte den WhatsApp Nutzer tatsächlich wegen eines rechtswidrigen Eingriffs in ihr Recht auf informationelle Selbstbestimmung abmahnen können.

Auch wenn das AG Bad Hersfeld wie oben geschildert einen Unterlassungsanspruch bejaht, kann man unter Berufung auf andere Urteile und die Literatur zu einem anderen Ergebnis kommen.

Besondere Relevanz ist hierbei dem Urteil des OVG Schleswig vom 09.10.2013 (Az. 8 A 37/12, 8 A 14/12, 8 A 218/11) zu schenken. Dieses sieht eine datenschutzrechtliche Verantwortlichkeit primär bei dem Betreiber des jeweiligen Mediums (in unserem Fall WhatsApp) und nicht bei den Nutzern selbst, wenn er faktisch keinen Einfluss auf die Datenerhebung und -verarbeitung hat.

Gegen eine rechtliche Verantwortlichkeit des privaten Nutzers würde zudem § 1 Abs. 2 Nr. 3 BDSG sprechen, wonach die Anwendbarkeit der Vorgaben des BDSG bei rein persönlichen oder familiäre Tätigkeiten ausgeschlossen sei.

Ein fahrlässiges Verhalten des Minderjährigen, erscheint zumindest fraglich, zumal der Minderjährige keine Kenntnis von der Datenweitergabe hatte.

Ob eine Welle von Abmahnungen daher zu erwarten ist bleibt abzuwarten und auch wie andere Gerichte in Zukunft ähnliche Fälle entscheiden werden (AG Bad Hersfeld, Beschl. v. 15.05.2017, F 120/17).

Artikel 29 Gruppe zur Verarbeitung von Arbeitnehmerdaten

Die Artikel 29 Gruppe, ein Gremium mit Vertretern aus den nationalen Datenschutzbehörden der Europäischen Union, hat eine neue Stellungnahme zur Verarbeitung personenbezogener Daten in Beschäftigungsverhältnissen veröffentlicht.

Da die alte Stellungnahme bereits aus dem Jahre 2001 stammt und die Verarbeitung personenbezogener Daten immer systematischer erfolgt, entschieden sie sich eine neue Stellungnahme zu veröffentlichen.

Der Begriff des Arbeitnehmers wird in der Stellungnahme weit ausgelegt, er umfasst sämtliche Personen, die einem Beschäftigungsverhältnis unterliegen und nicht nur solche die einen Arbeitsvertrag haben. Eingeschlossen werden damit unter anderem auch Selbstständige.

Des Weiteren werden in der Stellungnahme einige Verpflichtungen konkretisiert, die nach Ansicht der Artikel 29 Gruppe mit Inkrafttreten der Datenschutzgrundverordnung im Mai 2018 umzusetzen sind.

Aber warum genau ist eine neue Stellungnahme zum „klassischen“ Arbeitnehmerdatenschutz notwendig?

Zum einen ist dies darauf zurückzuführen, dass in der heutigen Zeit die Übergänge zwischen Privatleben und Arbeitszeit immer mehr verschwimmen. Unter anderem durch das Nutzen von Smartphones, Tablets oder Ähnlichem, sowohl privat als auch beruflich. Die Nutzung solcher Geräte erleichtern nicht nur den Arbeitsalltag vieler, sondern stellt auch häufig ein Risiko dar. Beispielsweise für auf den Geräten gespeicherte Kundendaten.

Zum anderen besteht weiterhin das Risiko, dass Arbeitnehmer durch ihren Arbeitgeber ungerechtfertigt überwacht werden. Egal ob bewusst oder unbewusst.

Genau diese Aspekte bewegten die Artikel 29 Gruppe dazu, eine neue Betrachtung zwischen den Interessen des Arbeitgebers und den Erwartungen des Arbeitnehmers durchzuführen.

Eine Verarbeitung personenbezogener Daten außerhalb der gesetzlichen Vorgaben im Verhältnis Arbeitgeber/Arbeitnehmer, lässt die

Artikel 29 Gruppe nur ausnahmsweise zu. Es muss dann eine freiwillige Einwilligung vorliegen, die jederzeit widerrufen werden kann.

Geraten wird den Arbeitgebern im Hinblick auf die Verarbeitung personenbezogener Daten sich zumindest im Rahmen einer datenschutzrechtlichen Prüfung über die Verhältnismäßigkeit der Datenerhebung zu informieren. Außerdem sind die Risiken der potentiellen Verletzung der Privatsphäre der Arbeitnehmer und des Kommunikationsgeheimnisses zu minimieren.

Die Artikel 29 Datenschutzgruppe stellt fest, dass Arbeitnehmer teilweise durch die zunehmende Digitalisierung in ihren Unternehmen enorm unter Druck gesetzt werden, insbesondere, da diesen die potentiellen Konsequenzen gegebenenfalls nicht bewusst sind. Gerade die Risiken für Arbeitnehmer durch die exzessive Sammlung von personenbezogenen Daten sieht sie als höchst problematisch an.

Zur Vermeidung von möglichen Problemen empfiehlt die Artikel 29 Datenschutzgruppe Arbeitgebern eine erhöhte Wachsamkeit im Umgang mit personenbezogenen Daten während der Verarbeitung. Die Verarbeitung muss notwendig sein und auf anwendbaren Rechtsgrundlagen basieren. Außerdem soll sie fair, verhältnismäßig gegenüber den vorgebrachten Anliegen und vor allem transparent für den Arbeitnehmer sein.

Die Stellungnahme fokussiert sich konkret auf sieben Szenarien.

Szenario 1 – Soziale Medien im Bewerbungsverfahren

- Kein Einholen von Informationen aus sozialen Medien im Bewerbungsverfahren (ausgenommen: XING, LinkedIn)
- Erhobene Daten sind bei Nichteignung des Bewerbers und Ablehnung sofort zu löschen
- Es besteht keine Rechtsgrundlage hinsichtlich Freundschaftsanfragen an den Bewerber oder sonstige Zugriffe auf deren Profilinhalte

Szenario 2 – Überwachung der Arbeitnehmer

- Die Sammlung von Informationen über die Arbeitnehmer mittels sozialer Medien ist per se irrelevant für das Beschäftigungsverhältnis
- Arbeitnehmer in besonderen Bereichen (Bsp. Pressesprecher) sollten nicht zur Nutzung eines vom Arbeitgeber bereitgestellten Profils verpflichtet werden
- Zugestanden wird dem Arbeitgeber eine Überwachung der LinkedIn Profile ausgeschiedener Mitarbeiter für die Dauer des nachvertraglichen Wettbewerbsverbots, um die Einhaltung des legitimen Arbeitgeberinteresses zu ermöglichen

Szenario 3 – Überwachung von Kommunikationstechnologien am Arbeitsplatz der Arbeitnehmer

- Eine Überwachung des Arbeitsplatzes ist nur in wenigen Fällen zulässig und damit auch verhältnismäßig
- Um die Nutzung bestimmter Internetseiten zu limitieren, wird empfohlen bereits im Voraus, präventiv, bestimmte Internetseiten zu blockieren

Szenario 4 – Überwachung von Kommunikationstechnologien fern des Arbeitsplatzes

- Insbesondere durch die Nutzung eigener technischer Geräte, dem Mobile Device Management und der Nutzung tragbarer Geräte kann das Privatleben der Arbeitnehmer einem stetig steigenden Risiko ausgesetzt sein. Es sollten bei einer solchen Nutzung immer auch die Risiken beachtet werden und notwendigerweise Sicherheitsvorkehrungen getroffen werden

Szenario 5&6 – Zeiterhebungen und Videoüberwachung

- Arbeitnehmer sind über jegliche Verarbeitun von Informationen (beispielsweise durch die exakte Erfassung von Ein- und Ausgangszeiten) zu informieren
- Verarbeitung für nicht verhältnismäßige Zwecke ist nicht erlaubt
- Von einer Nutzung automatisierter Gesichtserkennungstechnologien ist außer in wenigen Ausnahmefällen abzusehen, da diese als generell unverhältnismäßig gegenüber den Rechten und Freiheiten der Arbeitnehmer zu sehen ist

Szenario 7 – Überwachung von Firmenwagen

- Der Arbeitgeber ist verpflichtet die Arbeitnehmer über sämtliche Standortbestimmungsgeräte der Firmenwagen zu informieren.
- Bei erlaubter Privatnutzung des Firmenwagens außerhalb der Arbeitszeit besteht keine Rechtsgrundlage zur Überwachung der Standortdaten

Szenario 8&9 – Übermittlung von Arbeitnehmerdaten an Dritte im In- und Ausland

- Für die Übermittlung von Arbeitnehmerdaten an Dritte im Rahmen der Erbringung von Dienstleistungen besteht nach Ansicht der Artikel 29 Gruppe keine Rechtsgrundlage
- Jede Übermittlung von Daten ins nicht europäische Ausland bedarf eines angemessenen Schutzniveaus

Sämtliche vorstehenden Szenarien sind in einem datenschutzrechtlichen Gesamtkonzept zu berücksichtigen.

Hinweis:
Sollten Sie Hilfe bei der Sicherstellung eines angemessenen datenschutzrechtlichen Arbeitsverhältnisses haben, um im Zweifel Bußgeldern vorzubeugen, sprechen Sie uns gerne an.

SaphirIT GmbH
Sutthauser Straße 285
49080 Osnabrück
Geschäftsführer
Amtsgericht Osnabrück

www.saphirit.de
USt-ID-Nr. DE268765300
Frank W. Stroot
HRB 20385

Oldenburgische Landesbank AG
IBAN DE29 2802 0050 5042 8200 00
BIC OLBODEH2XXX

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