DOSB FÜHRUNGS AKADEMIE

FA Datenschutzportal

DSP Info-Brief

Nr. 50 / September 2017

INHALT

Herausgeber
Führungs-Akademie des DOSB

Kontakt FA
Führungs-Akademie des DOSB
Willy-Brandt-Platz 2 / 50679 Köln
Tel. 0221 – 221 275 94 /// Fax: 0221 – 221 220 13
www.fuehrungs-akademie.de
niewerth@fuehrungs-akademie.de

Technische Umsetzung
Führungs-Akademie des DOSB

Redaktion
Toni Niewerth / Robert Graf

Kontakt SVBG
Sachverständigenbürogemeinschaft Mülot:Graf
Westfalenweg 2
33449 Langenberg
www.muelot.de/
d.muelot@muelot-Graf.de

DATENSCHUTZPORTAL INTERN

1 Die Themen im Live-Chat vom 19.09.2017

1.1 Datenschutzrechtliche Einordnung zur Einführung einer Bewertungs-App für Schiedsrichter

Die Verantwortlichen im Schiedsrichterbereich des Verbandes haben – ohne den Datenschutzbeauftragten oder das Präsidium darüber zu informieren – eine sog. "Fairplay-App bei einer privaten Agentur in Auftrag gegeben und hatten diese auch bereits im Netz veröffentlicht.

Um den datenschutzrechtlichen Sachverhalt zu klären, wurde die Veröffentlichung aber erst einmal ausgesetzt und ich als Datenschutzbeauftragter auch beteiligt.

Worum geht es? - Informationen zur "App"

Die Bewertungs-App ermöglicht lediglich ein pauschales Bewerten in den Kategorien:

Exzellent /// Sehr gut /// Gut /// Ordentlich /// Zufriedenstellend /// Verbesserungswürdig /// Mangelhaft /// Inakzeptabel

Eine Kommentarfunktion gibt es nicht.

Die Daten der "App" befinden sich auf einer zentralen Internetseite bzw. den Servern der Entwicklungsfirma. Nur sie hat Zugriff auf die Daten.

Die Mitarbeiter dieser Firma haben entsprechende datenschutzrechtliche Verträge mit dieser Firma abgeschlossen.

Bewertungen (in den o.g. Kategorien) kann man nach der Anmeldung mit seiner E-Mail-Adresse abgeben.

Schiedsrichter, die nicht mitmachen, können nicht beurteilt werden. Inwieweit sie dadurch Nachteile haben, verschließt sich mir momentan noch.

Meine Fragen, bzw. Kommentierung, ob ich richtig liege:

FRAGE 1: Mit der Marketing-Firma muss ein entsprechender Vertrag zur Auftragsdatenverarbeitung und zum Datenschutz getroffen werden. Kann man das in einem Vertrag zusammenfassen?

FRAGE 2: Um zu beurteilen, welche Daten persönlichkeitsrechtlich relevant sind und welche Daten überhaupt Verwendung finden, ist das Erstellen eines Verfahrensverzeichnisses sowie einer Leistungsbeschreibung unumgänglich. Richtig?

FRAGE3: Ist richtig, dass von den betroffenen Schiedsrichtern eine schriftliche Einverständniserklärung vorliegen muss?

AW R. Graf
Ich gehe davon aus, dass der Dienstleister, der die App programmiert hat und zur Verfügung stellt, auch die genannte Marketingfirma in F1 ist.

Zu F1 und F2: Verantwortlich für die Verarbeitung ist der Verband. Die Daten werden bei der Marketingfirma gehostet und verarbeitet, also hier einen Auftragsdatenverarbeitungsvertrag abschließen. Die Regelungen in diesem Vertrag entsprechenden Regelungen zum Datenschutz. Wenn Sie meinen, dass es hier noch einen Dienstleistungsvertrag bedarf, dann ist auch dieser abzuschließen. Also noch einmal zusammengefasst: Der Dienstleistungsvertrag regelt die Dienstleistung, der Auftragsdatenverarbeitungsvertag regelt die datenschutzrechtlichen Aspekte. Und natürlich muss diese Verarbeitung personenbezogener Daten in das Verfahrensverzeichnis aufgenommen werden.

Bitte bedenken Sie, dass es bei dieser Verarbeitung zu einer Beurteilung von Personen kommt, d. h., dass eine Vorabkontrolle gemäß BDSG § 4d Abs. 5 durchgeführt werden muss: Eine Vorabkontrolle ist durchzuführen, wenn „die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens."

Zu F3: Ich würde auf jeden Fall eine schriftliche Einverständniserklärung einholen. In dieser Einverständniserklärung müssen die betroffenen Schiedsrichter auch gegebenenfalls über Konsequenzen einer solchen Beurteilung informiert und eine entsprechende Widerspruchsmöglichkeit ermöglicht werden.

Ich persönlich halte dieses Verfahren für heikel. Ich bin mir auch nicht sicher, ob in der gewählten Form des Verfahrens in ausreichendem Maße die besonderen Risiken für die Rechte und Freiheiten der Betroffenen berücksichtigt sind. Dagegen sprechen die nicht verifizierbare Anmeldemethode für diejenigen, die den Schiedsrichter beurteilen, und die Möglichkeit der App, einen Schiedsrichter in ein falsches Licht zu stellen.

1.2 Unberechtigte Weitergabe von Informationen durch ein Vorstandsmitglied an ein Vereinsmitglied

Nach der Weitergabe von Diskussionen aus Vorstandssitzungen und der Weitergabe von Vorstandsprotokollen an Dritte (Vereinsmitglieder, die nicht im Vorstand sind) ist im Vorstand eine Diskussion darüber entbrannt, ob das (namentlich bekannte) Vorstandsmitglied damit gegen das Datenschutzrecht verstoßen hat.

FRAGE: Ist der Vorwurf der Verletzung des Datenschutzrechtes richtig und kann ein solches Vergehen mit einer Abmahnung sanktioniert werden?

AW R. Graf
Diese Frage ist nicht ganz einfach zu beantworten. Es stellt sich zunächst die Frage, ob die Diskussion in Vorstandssitzungen und die Vorstandsprotokolle der Vertraulichkeit unterliegen.

Somit könnten möglicherweise datenschutzrechtliche Aspekte berührt sein, allerdings ist das auch von den im Verein festgelegten Regelungen abhängig. Daher möchte ich mich mit einer juristischen Beurteilung des Sachverhaltes zurückhalten und hier tatsächlich empfehlen, diese Frage von einem Juristen klären zu lassen. Da außerdem Fragen der Gestaltung der Vereinssatzung und der Anwendung des Vereinsrechts berührt werden, sollte auch zu diesen Fragen ein ausgewiesener Kenner dieser Bereiche kontaktiert werden.

1.3 Datenschutzrechtlich korrekte Information von Kadersportlern über Sonderkonditionen eines Sponsors

Der Verband hat einen Ausrüster für Kadersportler. Dieser möchte nun den Übungsleitern, Trainern und ehrenamtlich Tätigen ebenfalls über den Verband die Möglichkeit einräumen, zu reduzierten Konditionen für ihren Sport spezifische Kleidung bzw. Ausrüstungsgegenstände vom entsprechenden Ausrüster zu beziehen. Der Verband geht davon aus, dass viele der in Frage kommenden Personen das Angebot gerne nutzen möchten. Allerdings liegt dem Verband keine Einwilligung vor, die vorhandenen E-Mail-Adressen zu Werbezwecken zu verwenden. Eine Information dieses Personenkreises über das Weiterreichen der Konditionen per E-Mail verstößt daher wohl gegen §7 UWG.

FRAGE 1: Ist es richtig, dass die einzige Möglichkeit, sofern man nicht persönlich in Kontakt tritt, wie folgt aussieht: postalisches Anschreiben mit Erklärung des Sachverhalts und einer beiliegenden Einwilligungserklärung in ggf. zukünftige Verwendung der E-Mail-Adresse „zu Werbezwecken" (genaue Beschreibung wofür, Möglichkeit des Widerrufs etc.), die unterschrieben zurückgeschickt werden müsste bzw. ein Anschreiben mit einem Verweis auf eine Internetseite auf der eine Einwilligung „zu Werbezwecken" gegeben werden kann, verbunden mit double opt in?

FRAGE 2: Gibt es eine Möglichkeit in allgemeiner Form darüber zu informieren, dass es „entsprechende Vergünstigungen/Konditionen" aufgrund der Zugehörigkeit zum Verband gibt/ geben könnte und dass bei Interesse, "konkrete werbliche Informationen zu erhalten" z. B. eine Registrierung auf einer Internetseite (DOI) bzw. eine wie auch immer geartete Einwilligung gegeben werden müsste?

FRAGE 3: Darf ein Verein im Rahmen eines regelmäßig erscheinenden Newsletters auf solche Möglichkeiten hinweisen, verbunden mit dem Verweis, dass er diese an seine Mitglieder/ Trainer weiterreichen darf, sofern er eine entsprechende Einwilligung hat. Kann dies auch als Info auf einer Mitgliederversammlung verkündet werden?

AW R. Graf:
Zu F 1: Die Weitergabe der Übungsleiternamen und Adressen an den Ausrüster ist ohne Einwilligungserklärung – wie schon vermutet – nicht möglich.

Der Verband kann allerdings, da er die E-Mail Adressen seiner Übungsleiter ja hat, diese durchaus über die Möglichkeiten informieren. Dann können die Übungsleiter und Sportler sich selbst an den Ausrüster wenden. Auch können hier Newsletter und Webseite des Verbandes genutzt werden, um diese Information an die Übungsleiter und Sportler weiterzugeben.

Nach Gola (Kommentar zu Bundesdatenschutzgesetz) ist für Werbezwecke ohne Einwilligung die adressierte Briefwerbung erlaubt für eigene oder gegebenenfalls in Form der Beitrags- oder Empfehlungswerbung für fremde Ziele, wenn sie sich an sogenannte Bestandskunden richtet, d. h. Betroffene mit denen zumindest ein rechtsgeschäftsähnliches Schuldverhältnis begründet besteht oder bestand.

Meiner Meinung nach ist das hier aber nicht ein Fall der Werbung, sondern sie informieren ja eigene Übungsleiter und Sportler.

Zu F2 und F3: Meine oben gemachten Ausführungen machen meiner Meinung nach diese Fragen hinfällig. Wenn ich die Frage richtig verstehe, wendet sich der Verband an eigene

Übungsleiter und Sportler. Wenn es darum geht, dass der Verband diese Möglichkeit seinen Vereinen und deren Übungsleiter und Sportler anbieten möchte, wäre es einfacher, wenn der Verband die Vereine informiert und die Vereine dann ihre eigenen Übungsleiter.

1.4 Weitergabe eines Vereinsbriefkopfes an ein Mitglied, das damit die Abwahl eines Vorstandsmitgliedes beantragen möchte

Nach der Weitergabe des Vereinsbriefbogens mit Briefkopf als Datei durch den Vereinsvorsitzenden an ein Vereinsmitglied ist dem Vorsitzenden der Vorwurf gemacht worden, gegen das Datenschutzrecht verstoßen zu haben.

Frage: Ist die Weitergabe des Vereinsbriefbogens an ein Vereinsmitglied ein Verstoß gegen das Datenschutzrecht?

AW R. Graf: Ich gehe davon aus, dass es sich bei dem Briefbogen um den offiziellen Vereinsbriefbogen handelt, der als Standardbriefbogen u.a. auch zur allgemeinen Kommunikation des Vereins, z.B. mit Mitgliedern, Kunden, Funktionsträger, Lieferanten etc., genutzt wird. In diesem Fall gelten die dort abgedruckten Personendaten als öffentliche Daten, weil sie einem größeren Personenkreis bekannt sind. Darüber hinaus sind die auf dem Briefbogen enthaltenen Namen des Vereinsvorsitzenden bzw. des Vorstandes über das Vereinsregister öffentliche Daten. Ich sehe hier daher keinen Datenschutzverstoß.

SAVE THE DATE

Der nächste Live-Chat findet am Freitag, den 27. Oktober, 09:00 Uhr – 10:00 Uhr, statt.

Fragen, die vorab an die E-Mailadresse ds-communicator@fuehrungs-akademie.de oder an niewerth@fuehrungs-akademie.de gesendet werden, stelle ich in allgemeiner Form – ohne konkreten Bezug zum Verein / Verband unter dem Nutzernamen ds-communicator in den Live-Chat ein. *[TN]*

2 Neue Dokumente im Portal

Zur Unterstützung Ihrer Vorbereitungen zur Anwendung der EU-DSGVO ab Mai 2018 und des im Sommer verabschiedeten neuen Bundesdatenschutzgesetz (BDSG NEU) werden zurzeit zahlreiche Dokumente überarbeitet und in den kommenden Wochen neu eingestellt. Wir beginnen die Neueinstellung und Aktualisierung, indem wir Ihnen die aktuelle Seminar-Schulungsunterlage zur EU DSGVO unter der Rubrik „Schulungen" zur Verfügung stellen.

IN DER DISKUSSION – AKTUELLES RUND UM DEN DATENSCHUTZ

3 Die Beseitigung der WLAN-Störerhaftung

- Ein Lernprozess für den Gesetzgeber – Fortsetzung folgt?
- Beitrag von Professor Achim Albrecht, Westfälische Hochschule, Gelsenkirchen,
- *Quelle: veröffentlicht in: Richard-Boorberg-Verlag : PUBLICUS, Der Online Spiegel für das öffentliche Recht, Ausgabe 2017-09 vom 19.09.2017*
-

Der Problemkreis

Noch vor zwei Jahren äußerten sich der EuGH und nationale Gerichte im Umfeld von Urheberrechtsverletzungen durch Cyberkriminalität mit recht unterschiedlicher Argumentation zu den möglichen rechtlichen Verantwortlichkeiten der Beteiligten.

Einig war man sich darüber, dass grundsätzlich immer der Verursacher solcher Rechtsverletzungen als typischer Handlungsstörer auf Unterlassung und Schadensersatz in Anspruch genommen werden kann. Allerdings: Berechtigte Ansprüche scheiterten fast durchweg daran, dass man weder Firmen noch handelnde Personen ausfindig machen oder gar in Anspruch nehmen konnte – handelten diese doch oft in völliger Anonymität unter der Verwendung von Deckadressen und aus der Sicherheit exotischer Lokationen heraus.

Also verfiel man auf die Idee, subsidiär und im Rahmen des Verhältnismäßigkeitsgrundsatzes bei genau diesen Konstellationen die sogenannten Zustands- oder Vermittlungsstörer – nämlich die Netzprovider im erreichbaren Inland – in Anspruch zu nehmen. Diese hatten zwar lediglich für den Netzzugang gesorgt und arbeiteten auch nicht kollusiv mit den Rechteverletzern zusammen. Dennoch schrieb man ihnen zu, dass ohne die Schaffung eines Netzzuganges keine Rechtsverletzung möglich gewesen wäre, eine reine Äquivalenzüberlegung also.

Die Provider, so folgerte man, könnten als faktische Vermittlungs- und Zustandsstörer subsidiär auf Sperrung eines in krimineller Weise gebrauchten Accounts in Anspruch genommen werde, wenn zumutbare Bemühungen nachweisbar scheiterten, die gut getarnten Handlungsstörer zur Verantwortung zu ziehen.

Eine weitere, noch weitreichendere Facette der Verantwortlichkeiten rund um die Störerhaftung bei Cyberkriminalität, war die Verantwortlichkeit für den Missbrauch von WLAN-Netzen. Mit der immer weiter voranschreitenden Abdeckung von Haushalten, Unternehmen und öffentlichen Flächen durch WLAN-Zugangsmöglichkeiten musste auch diskutiert werden, wer für typische Rechtsverletzungen unter Verwendung eines WLAN-Zugangs, der einem Betreiber zugeordnet wurde, zur Verantwortung gezogen werden konnte. Zunehmend häufig loggten sich Rechtsverletzer zum Upload oder Download von Materialien in fremde Netze ein, um Urheberrechtsverletzungen und andere Straftaten zu begehen und sich anschließend ohne zurückverfolgbare Spur auszuloggen. Zurück blieb der ahnungslose WLAN-Betreiber, dessen Kennung eine unverwechselbar verfolgbare Spur hinterließ: auch hier eine 2.0 Version der Verantwortlichkeitshierarchie »sichtbarer Zustandsstörer versus getarnter Handlungsstörer«.

Die Gerichte bemühten sich um einen fairen Interessenausgleich zwischen Geschädigten und potenziellen Schädigern und gaben den WLAN-Betreibern auf, ihre Netze in zumutbarem Umfang zu sichern und zu verschlüsseln, um einen allzu leichten Zugang für jedermann zu stoppen. Sogleich entbrannte eine Diskussion darüber, was eine »zumutbare und sichere Verschlüsselung« sei. Was passiere, wenn Restaurants und Friseure, private Haushalte bei Einladungen und Behörden ihren Besuchern die Passwörter zu ihrem WLAN aushändigten, und damit die Sicherheitsmaßnahmen durch Weitergabewellen erodiert würden? Müsse in solchen Fällen in schnellem Rhythmus das Passwort geändert werden?

Fragen über Fragen, die eine Fülle von Einzelentscheidungen zu provozieren drohten.

Die erste Maßnahmerunde

Nach langer Diskussion entschloss sich der Gesetzgeber im Jahr 2016, durch eine Änderung des Telemediengesetzes (TMG) die Rechtsunsicherheit rund um die WLAN-Störerhaftung zu beenden.

Rechtspolitisch entschied man sich dafür, die extensive Störerhaftung zugunsten der dringend notwendigen flächendeckenden Netzabdeckung zu kappen. Im Klartext bedeutet dies, dass es auch bei unverschlüsselten, für Jeden erreichbare Hotspots, nicht zu einer Betreiberhaftung bei Missbrauchsfällen durch Dritte kommen sollte. Damit wähnten sich zunächst die Anbieter von Hotspots sicher, weil sie nicht mehr wie bisher für das Verhalten ihrer Nutzer haften sollten. [LINK zum vollständigen Text]

MEDIEN –TECHNIK – SICHERHEIT

4 WhatsApp im Nutzungscheck

Stellungnahme der Datenschutzauditorin Eva-Daniela Jung zur Nutzung von WhatsApp

Was genau ist WhatsApp?

WhatsApp ist eine werbefreie, plattformübergreifende mobile Nachrichten App, die es erlaubt, Nachrichten auszutauschen, ohne für SMS zahlen zu müssen. WhatsApp läuft auf allen gängigen Smartphones und ist für die Übermittlung von Text, Bild- und Tonnachrichten als auch Standortdaten geeignet. Seit dem Frühjahr 2015 ist ebenso das internetbasierte Telefonieren über die App möglich.

Da der WhatsApp Messenger den Datentarif verwendet, der auch für E-Mails und mobiles Surfen im Internet genutzt wird, ist es kostenlos, Nachrichten zu verschicken. Außerdem ist es möglich Gruppen zu erstellen.

Der im Jahre 2014 von Facebook gekaute Instant-Messaging-Dienst ist somit eine der meist genutzten Plattformen im Netz und stellt die nächste Stufe der Evolution in der Kommunikation da. Eine tolle Sache – die Zielgruppe ist immer und überall erreichbar – ein Traum wird wahr! Noch näher konnte man nie an der Zielgruppe sein. Den Klienten immer und überall erreichen – endlich ist das möglich! Dank WhatsApp.

Bedeutung

Wir wollen alle jung, hip und innovativ sein. Und dann gibt es da noch diese ominöse Generation Y, von der alle sprechen. Und sie sind doch alle da, die sind alle mobil, die sind auf WhatsApp und aktivieren ihr Smartphone 135-mal am Tag. Tatsächlich, ungeachtet NSA-Skandal und Datenschutzbedenken ist alle Welt auf WhatsApp – dem weltweit meist genutzten Messenger Dienst.

Wo ist der Hacken?

Abgesehen von einer fehlenden End-zu-End-Verschlüsselung[1], wird WhatsApp immer wieder wegen seinen allgemeinen Geschäftsbedingungen kritisiert. So erlauben diese dem Unternehmen, Medien der Nutzer zu kommerziellen Zwecken zu nutzen.

---

[1] Eine End-zu-End-Verschlüsselung wird seit April 2016 angeboten: „*Wir bieten außerdem eine Ende-zu-Ende-Verschlüsselung für unsere Dienste an, die standardmäßig aktiviert ist, wenn du und die Personen, mit denen du chattest, eine Version unserer App verwenden, die nach dem 2. April 2016 veröffentlicht wurde. Ende-zu-Ende-Verschlüsselung bedeutet, dass deine Nachrichten verschlüsselt sind, um davor zu schützen, dass wir oder Dritte sie lesen können. [Quelle]*

Kritiker weisen allerdings immer wieder auf die Schwachstellen dieses Angebots hin. Als ein Beispiel sei die Stellungnahme des Sicherheitsexperte Cris Thomas zitiert, der zu darauf die Inhalte damit „'lediglich' auf dem Weg von einem Smartphone zu dem anderen geschützt sind. Die Daten auf den Smartphones selbst" bleiben, so Thomas, „weiterhin vollkommen ungeschützt. Das gilt besonders, wenn Sie Ihre Chats in einer unverschlüsselten Cloud sichern oder Dritten Zugang zu Ihrem Smartphone gewähren." [LINK zum vollständigen Artikel]

Auch liegen die allgemeinen Geschäftsbedingungen trotz richterlicher Anordnung vom Landgericht in Berlin im Jahr 2014 nach wie vor nur in englischer Sprache vor.

Im Mai 2012 kritisierte die Stiftung Warentest das Datensendungsverhalten der App, da diese alle gespeicherten Telefonnummern (die bei WhatsApp als Nutzerkennungen dienen) unverschlüsselt an den WhatsApp-Server überträgt, und vergab das Urteil „sehr kritisch". Auch in einem Schnelltest im Februar 2014 erhielt die App das Urteil „sehr kritisch" im Bereich Datenschutz.

Im April 2015 wurde bekannt, dass WhatsApp in der Version 2.12.45 alle über die App geführten Anrufe ungefragt mitschneidet und im lokalen Speicher aufhebt.

Im Juni 2015 wurde erstmals offiziell bekannt, dass amerikanische Behörden die Möglichkeit haben, WhatsApp-Nachrichten mitzulesen.

Gewerbliche Nutzung von WhatsApp

Was sagen uns die Nutzungsbedingungen von WhatsApp?

> *„You agree not […] to use the communication systems provided by the Service for any commercial solicitation or spam purposes. You agree not […] to solicit for commercial purposes, any users of the Service.*"

Dort steht eindeutig, dass die Nutzung für gewerbliche oder kommerzielle Zwecke nicht erlaubt ist, bzw. dass Sie zustimmen, WhatsApp nicht für diese Zwecke zu missbrauchen.

Weiter heißt es:

> *„In connection with Status Submissions, you further agree that you will not: […] (iv) post advertisements or solicitations of business.*"

Zum einen schützt Unwissenheit vor Strafe nicht, zum anderen sollte ein Unternehmen, das über die Nutzung von WhatsApp nachdenkt, schon ganz genau hinschauen, ob das denn überhaupt mit den Nutzungsbedingungen (oder gar dem deutschen Recht) vereinbar ist.

Schauen wir aber mal großzügig über die beiden Paragraphen hinweg. Was ist dann der nächste Stolperstein? Wie heißt es so schön?

> *„You agree not to collect or harvest any personally identifiable information, including phone number, from the Service, nor to use the communication systems provided by the Service for any commercial solicitation or spam purposes.*"

Mit Annahme der Nutzungsbedingungen stimme ich also zu, keine persönlichen Daten zu sammeln. Hm. So ein Gruppenchat mit bis zu 100 Kunden/Klienten? Macht 100 Daten, die ich sammeln könnte.

Und weiter:

> *„You expressly acknowledge and agree that in order to provide the Service, WhatsApp may periodically access your contact list and/or address book on your mobile device to find and keep track of mobile phone numbers of other users of the Service. […]. You hereby give your express consent to WhatsApp to access your contact list and/or address book for mobile phone numbers in order to provide and use the Service.*"

Damit WhatsApp auch in den nächsten Jahren seinen Service verbessern kann, erlaubt man sich dort hin und wieder, ab und zu mal auf die Kontaktliste bzw. das Adressbuch

zuzugreifen. Und damit quasi auch auf die Kontakte aus Ihrem Gruppenchat. Wann das Ganze passiert, weiß ja kein Mensch. Durchaus möglich also, dass das in dem Moment geschieht, wenn Sie Ihren Kunden-Chat abhalten. Datenschutzkonform ist das definitiv nicht.

Zu guter Letzt:

> *„By submitting the Status Submissions to WhatsApp, you hereby grant WhatsApp a worldwide, non-exclusive, royalty-free, sublicenseable and transferable license to use, reproduce, distribute, prepare derivative works of, display, and perform the Status Submissions in connection with the WhatsApp Service and WhatsApp's (and its successor's) business, including without limitation for promoting and redistributing part or all of the WhatsApp Service (and derivative works thereof) in any media formats and through any media channels. You also hereby grant each subscriber to your status on the WhatsApp Service a non-exclusive license to access your Status Submissions through the Service.*"

Damit übertragen Sie WhatsApp alle Rechte, über Ihre Meldungen zu verfügen! WhatsApp ist quasi Alleinherrscher über das, was Sie da Tag für Tag, Stunde für Stunde, Minute für Minute, Sekunde für Sekunde von sich geben.

Was sagt ein Rechtsexperte?

Carsten Ulrich (Rechtsanwalt für u.a. Internet und Social Media) auf dem Block Recht 2.0

> *„Die rechtliche Zulässigkeit des Einsatzes von WhatsApp für die Kundenkommunikation, insbesondere im Bereich Service und Support, hängt stark vom konkreten Szenario ab. Während sich das Angebot einer Erreichbarkeit über WhatsApp bei Beachtung der aufgeführten Voraussetzungen durchaus rechtskonform aufsetzen lassen dürfte, ist etwa die werbliche Ansprache von Kunden auf WhatsApp bzw. das Verlagern der kompletten Kommunikation mit einzelnen Kunden auf einen entsprechenden Kanal, der in datenschutzrechtlicher Hinsicht immer wieder diskutiert wird, durchaus problematisch.*"

Er empfiehlt „Unternehmen, die sich trotz der anhaltenden Zweifel an der Rechtskonformität und Sicherheit von WhatsApp die spannenden Möglichkeiten der Kundenkommunikation über Mobile Messenger nicht nehmen lassen wollen, sollten sich nach alternativen Anbietern umsehen, die nicht nur den Anforderungen an das deutsche Datenschutzrecht genügen, sondern den Unternehmen auch die anzustrebende Kontrolle über die Verarbeitung und Nutzung der Daten einräumen."

Empfehlung durch den Datenschutzbeauftragten

Finger weg von WhatsApp für die gewerbliche Nutzung!

Die möglichen Verstöße gegen die WhatsApp-Nutzungsbedingungen sind aber eigentlich nur Peanuts. Viel gravierender ist nämlich die (daraus resultierende) Datenschutzproblematik. Und die fängt schon damit an, dass der Sitz von WhatsApp in Kalifornien liegt. Weit weg von uns auf einem US-amerikanischen Server liegen also all die Daten, die da im Rahmen eines Kunden-/Klienten-Chats gesammelt wurden. Ohne jede Zugriffsmöglichkeit durch Sie. Ohne dass irgendeiner der Klienten was davon weiß. Und dann die Sache mit den personenbezogenen Daten (sprich Telefonnummern). Denn hier hatte nicht nur das Unternehmen Einblick, sondern (zumindest zeitweise immer mal wieder) jeder Nutzer des Chats.

Was kann passieren?

Die wahrscheinlich schlimmste Konsequenz seitens WhatsApp ist die, dass Ihr Account gelöscht wird. Und zwar ohne jede Voranmeldung. Viel schwer wiegender ist, dass bis zu 300.000 Euro Bußgelder drohen, wenn gegen das Bundesdatenschutzgesetz verstoßen wird.

Quellen

www.Rechtzweinull.de /// www.personalmarketing2null.de /// www.Computerwoche.de /// www.it-recht-kanzlei.de /// www.wbs-law.de /// www.e-recht24.de /// www.ihr-law.de [EDJ, Ersterstellung Febr. 2016J

Weiterführende Hinweise zum Thema WhatsApp

(vgl. auch die Rubrik „Urteile" in dieser Ausgabe des Info-Briefes)

- WhatsApp – eine Bestandsaufnahme [Datenschutzhelden] [16.08.17]
- WhatsApp: Ist es legal, WhatsApp in Deutschland zu benutzen? [Die Zeit online] [27.06.17]
- Weitergabe von Kontaktdaten an WhatsApp unzulässig [FR online] [29.06.17]
- Datenschutz: WhatsApp an der Schule - was geht, was nicht? [Spiegel Online] [24.04.17]
- WhatsApp an Schulen: Was ist erlaubt?– Forum – [Spiegel Online]
- Datenschutzbeauftragter warnt vor WhatsApp & Co. an Schulen [Heise Online] []07.05.2017
- Diese WhatsApp-Sicherheitslücke ist eine Einladung für Kriminelle [Die Welt / N 24] [13.05.17]
- WhatsApp: Datenschutz trotz Verschlüsselung kritisch [Verbraucherzenrale NRW] [11.04.17]
- Was Facebook mit Ihren Whatsapp Daten vorhat [SZ Online] [18.05.17]
- WhatsApp-Alternativen: die Datenschutzregeln im Überblick [Verbraucerzentrale NRW] [31.01.2017]

[Zusammenstellung und Auswahl:TN]

GESETZGEBUNG

5 Die EU DSGVO im Sport – Interview mit Dirk Michael Mülot

Übernahme aus dem FA-Newsletter Nr. 68. August / September 2017

RED:
Datenschutz und Datensicherheit spielen auch im Sport eine immer größere Bedeutung. Neben einzelnen Bereichen in denen beispielsweise sensible Gesundheits- und Leistungsdaten bearbeitet werden, hat der Datenschutz mittlerweile fast alle Ebenen der Vereins- und Verbandsarbeit durchdrungen.

Herr Mülot, Sie sind bundesweit sowohl in der freien Wirtschaft als auch im Sport agierender Datenschutzbeauftragter und Dozent für zahlreiche Seminare rund um das Thema Datenschutz. Hier sehen Sie sich tagtäglich mit Fragen der Akzeptanz und der Umsetzung des Datenschutzes konfrontiert: Wie schätzen Sie die aktuelle Situation des Datenschutzes im Sport ein? Ist der Datenschutz im Sport angekommen?

D. M. Mülot:
Es hat schon einen Ruck gegeben. Das merken wir an zunehmenden Anfragen in unserem Büro aus den gesamten Bereichen des Sports, ob von Vereinen oder Verbänden, weil die Vorstände und Geschäftsführungen immer mehr für das Thema sensibilisiert werden und man den Handlungsbedarf immer mehr erkennt. Denn gerade der Startschuss der Datenschutzgrundverordnung (DSGV), die am 25. Mai 2018 rechtskonform in allen Einrichtungen umgesetzt werden muss, erhöht seitens der Vorstände und der Geschäftsführungen den Leidensdruck und geht mit einem Handlungsbedarf einher. Ich stelle fest, dass sich die Sportorganisationen mehr und mehr Gedanken darüber machen, wie sie diesen Anforderungen bis Mai 2018 gerecht werden können.

RED:
Mit der 2016 vom EU-Parlament beschlossenen und ab Mai 2018 in vollem Umfang auch in Deutschland anzuwendenden EU Datenschutzgrundverordnung (DSGV) ist also neue Bewegung ins Spiel gekommen. Viele Datenschützer sind ebenso wie die verantwortlichen Vorstände und Geschäftsführungen verunsichert, was die DSGV für den eigenen Verein bzw. Verband bedeutet. Wer ist von dieser Gesetzgebung betroffen und was sind aus Ihrer Sicht die wichtigsten Neuerungen gegenüber den bisherigen Regelungen des Bundesdatenschutzgesetzes (BDSG)?

D. M. Mülot:
Ja, es ist Bewegung ins Spiel gekommen. Durch die DSGV sind die Strafen deutlich höher aufgehängt worden, als dies bisher im BDSG der Fall war und das führt zu Handlungsnot, denn hier drohen Strafen in Höhe von 2 % bis 4 % des Jahresumsatzes bzw. 10 bis 20 Mio. EUR. Ich denke, man sollte es an dieser Stelle nicht überbewerten, nichtsdestotrotz sind das natürlich Summen, die für Vereine und Verbände unter Umständen existenzbedrohend sein können.

Von den neuen Regelungen betroffen sind natürlich zunächst einmal die Geschäftsführung, die Vorstände sowie jeder einzelne Mitarbeiter, jede einzelne Mitarbeiterin. Denn sie sind letztendlich diejenigen, die Datenschutz im operativen Tagesgeschäft realisieren und sich an die Vorschriften halten müssen. Wir haben hier einerseits die DSGV und die sogenannten Anpassungsgesetze, das neue BDSG beispielsweise, das ebenfalls mit Wir-

kung zum 25. Mai 2018 eintritt und weiterhin die Landesdatenschutzgesetze (LDSG), die noch nicht veröffentlicht sind und aktuell in der Entwicklung stehen.

Eine wichtige Neuerung, die die Einführung der EU-DSGV mit sich bringt ist folgende: Bisher musste man nur den Nachweis erbringen, dass man etwas getan hat im Bereich des Datenschutzes und die vorgegebenen Gesetze einhält. Mit der neuen Gesetzgebung muss nun zukünftig jede Einrichtung, also jeder Verein/Verband anhand von beschriebenen Prozessen und mit geltenden Dokumenten nachweisen, wie genau sie die Einhaltung der Regelwerke sicherstellt.

Die detaillierte, saubere Dokumentation dieser Prozesse ist sicherlich eine der größten Herausforderungen, die jetzt auf die Sportorganisationen zukommt.

Das bedeutet zwar deutlich mehr bürokratischen Aufwand, aber ist mit Blick auf die Zielrichtung der DSGV durchaus wichtig. Denn beim Datenschutz geht es nicht – wie meist irrtümlich angenommen – um den Schutz der Daten, sondern darum, den Betroffenen davor zu schützen, dass ihm durch die Erhebung, Verarbeitung und Nutzung seiner Daten ein Nachteil entsteht. Bisher haben die Organisationen meist den Fokus auf den eigenen Schaden gelegt, der ihnen möglicherweise entstehen kann, wenn sie sich nicht an Regelwerke halten. Dies muss im Rahmen der DSGV komplett neu gedacht werden. Die DSGV betrachtet den Datenschutz immer aus Sicht des Betroffenen: Was geschieht beispielsweise, wenn Gesundheits- oder Leistungsdaten unberechtigterweise Dritten zur Kenntnis gelangen? Welcher Schaden kann dem Betroffenen entstehen? Das bedeutet im Umkehrschluss, dass wir anhand von Verfahrensbeschreibungen, die eigentlich auch schon aus dem alten Gesetz heraus vorliegen sollten, letztendlich zu jedem Verfahren auch eine so genannte Datenschutzfolgenabschätzung durchführen müssen, um zu prüfen, welche Risiken bei Verlust von Vertraulichkeit, Verfügbarkeit und Integrität für den Betroffenen auftreten. Dadurch wird der Aufwand natürlich etwas umfangreicher.

RED:
Neben diesen neuen Gesetzen, die wir gerade diskutiert haben, sind ab 2018 auch landesweite Einzelregelungen im Datenschutzrecht angedacht. Die EU möchte mit diesen Öffnungsklauseln den nationalen Parlamenten die Möglichkeit geben, bestehende Datenschutzgesetze in die EU-Datenschutzgrundverordnung zu integrieren. Diese machen das Gesetz flexibler und in den Ländern auch leichter durchsetzbar. Wird damit aber nicht zugleich auch die Chance vertan, eine tatsächlich europäisch einheitliche Datenschutzgesetzgebung durchzusetzen?

D. M. Mülot:
Man hatte in der Vergangenheit anhand einer so genannten EU Datenschutzrichtlinie den Wunsch, dass sich die einzelnen Länder anhand der Richtlinie mit eigenen Datenschutzgesetzen versehen, um diese Regelwerke entsprechend einhalten zu können. Dabei handelte es sich allerdings nur um eine Richtlinie, d.h. sie war nicht verpflichtend.

Wir in Deutschland haben daraufhin ein Bundesdatenschutzgesetz, ein Landesdatenschutzgesetz und auch kirchliche Datenschutzgesetze entwickelt, die dieser Richtlinie entsprochen haben. Einige Länder haben dies nicht getan, z.B. Irland. Und in diesen Fällen hat es eine klare Wettbewerbsverzerrung gegeben und keine Wettbewerbsgleichheit mehr, denn in Deutschland mussten sich die Unternehmen mit dem Thema Datenschutz auseinandersetzen. Das verursachte Kosten und Aufwände und führte auch dazu, dass einige Prozesse, gerade im Bereich Marketing und Werbung, nicht mehr möglich waren.

Das war auch einer der Gründe, weshalb sich z.B. Callcenter-Betriebe im Bereich von Werbemaßnahmen oder Direktvermarktung in Länder wie Irland abgesetzt haben, um von dort aus entsprechend agieren zu können.

Die DSGV, die sofort geltendes Gesetz in allen Ländern ist, ohne dass diese ein eigenes Gesetz haben müssen, fordert jetzt alle Beteiligten dazu auf, sich an dieses Grundregelwerk zu halten. Die Eröffnungsklauseln besagen, dass ein Land, das vor Inkrafttreten der EU Grundverordnung eigene Regelwerke hatte, diese noch weiter verfeinern kann. Diese Landesgesetze werden dann auch entsprechend akzeptiert. Die vorhandenen Bundesdatenschutz- oder Landesdatenschutzgesetze oder die Gesetze, die einzelne Länder, wie Italien oder Frankreich jetzt noch ins Leben rufen werden, können nur noch weiter verfeinert, jedoch die Grundregeln der DSGV nicht aufgebrochen werden.

Das ist also das Mindestrahmenwerk, das eingehalten werden muss. Gerade im Kontext der zunehmenden Digitalisierung ist es aus meiner Sicht durchaus sinnvoll, einen einheitlichen Mindestschutzbedarf für die Betroffenen in allen Ländern zu gewährleisten.

Nehmen wir ein einfaches Beispiel: Die DSGV schreibt ab gewissen Risikoklassen oder verarbeiteten Datenmengen die Bestellung eines Datenschutzbeauftragten vor. Im neuen Bundesdatenschutzgesetz hat man dieses alte Regelwerk beibehalten, das bereits vor der DSGV existierte und dieses noch verfeinert. So gilt in Deutschland, dass Organisationen, in denen mehr als neun Mitarbeiter/-innen, die in ihrer beruflichen Tätigkeit mit personenbezogenen Daten in Kontakt kommen, also Daten erheben, verarbeiten oder mittels elektronischer Datenverarbeitung nutzen, einen Datenschutzbeauftragten bestellen müssen (dies gilt übrigens auch für ehrenamtlich im Verein/Verband Tätige).

Man hat hier die Latte also noch ein wenig höher gehängt. Ich halte das für sehr sinnvoll, denn für viele Organisationen ist der Datenschutz ein noch relativ unbekanntes Thema, gerade, wenn es um die Feinheiten geht. Hier bedarf es einen Datenschutzbeauftragten, der die Grundregeln des Datenschutzes kennt und den Vorstand sowie die die Mitarbeiter entsprechend im Umgang mit personenbezogenen Daten beraten kann.

Die Bestellung eines Datenschutzbeauftragten wird in den meisten Vereinen und Verbänden unabwendbar sein. Darüber sollte sich jede Organisation Gedanken machen. Denn die bereits erwähnten Regelungen betreffen auch ehrenamtlich Tätige, die mit personenbezogenen Daten arbeiten, wie beispielsweise Übungsleiter oder Jugendwarte. Vereine und Verbände sind daher gefordert, erst einmal eine Auflistung zu machen, wer Zugang und Zugriff auf die personenbezogenen Daten bekommt und zu welchem Zweck.

Red.:
Im Mai haben Bundesrat- und Bundestag mit der Verabschiedung des Datenschutz-Anpassungs- und Umsetzungsgesetzes eben genau diese deutsche Version des neuen Datenschutzgesetzes beschlossen. Was sind die Kernelemente des Gesetzes und gibt es Vorgaben, auf die Vereine und Verbände besonders achten sollten?

D. M. Mülot:
Eigentlich müssen die Vereine und Verbände auf alle Vorgaben achten. Ich empfehle jedoch, sich nicht nur auf das BDSG Neu oder auch die neuen Landesdatenschutzgesetze (LDSG) zu stürzen, sondern erst einmal die Anforderungen, die die DSGV stellt, zu gewährleisten und dann zu schauen, welche Verfeinerungen es im BDSG oder im LDSG gibt und diese dann entsprechend anpassen.

Ein Beispiel: In der DSGV werden die technisch-organisatorischen Maßnahmen in Bezug auf die Sicherheit der Datenverarbeitung lediglich in einer kurzen Definition aufgeführt. Im BDSG sind die technisch-organisatorischen Maßnahmen in 14 Punkte aufgelistet, die von jeder Einrichtung zu erfüllen sind, um die Sicherheit in der Verarbeitung entsprechend sicherzustellen.

Red.:
Der Aufwand, den Sportvereine und –verbände kalkulieren müssen, um die neuen Vorgaben der EU-DSGVO und des Anpassungsgesetzes des Bundestages im eigenen Verein / Verband umzusetzen, ist sicher unterschiedlich und sehr stark vom aktuellen Status des Datenschutzes und der bisherigen Tätigkeit in diesem Feld abhängig. Was müssen aus Ihrer Sicht Vereine und Verbände unternehmen, um die Forderungen der neuen Datenschutzgesetzgebung bis Mai 2018 umzusetzen? Was könnten erste Schritte sein, um den konkreten Aufwand zu ermitteln?

D. M. Mülot:
Zunächst einmal gilt es, Strukturen und Prozesse in der Organisation anzupassen. Es müssen Prüfprozesse installiert werden, die festlegen, wie und von wem die Rechtmäßigkeit der Datenverarbeitung geprüft wird. Diese Strukturen und Prozesse müssen dann genau beschrieben und dokumentiert werden. Gleiches gilt für die Festlegung der Rechtsgrundlagen und der Zwecke der Datenverarbeitung sowie deren Dokumentation. Nehmen wir das Beispiel der Lizenzvergabe eines Spielers. Hier müssen die entsprechenden Rechtsgrundlagen vorliegen, die es zu erfüllen gilt und es muss geklärt sein, welche Daten in welchem Zusammenhang erhoben, verarbeitet und genutzt werden dürfen.

Der zweite große Block ist dann die Implementierung von Informationspflichten und die Sicherstellung der Betroffenenrechte sowie der Aufbau von entsprechenden Löschkonzepten. Die Betroffenen haben ein Recht auf Datenkorrektur, auf Löschung, auf Auskunft, das Recht auf Vergessenwerden usw.. Hierzu muss es entsprechende Prozesse geben, die sicherstellen, dass die Rechte der Betroffenen eingehalten werden. Das Ganze erfolgt unter dem Oberbegriff „Intervenierbarkeit". Es muss also dokumentiert werden, wie der Verein/Verband sicherstellt, dass die Betroffenen ihre Rechte wahrnehmen und auch durchsetzen können.

In einem nächsten großen Block muss die Anpassung der Datenschutzorganisation in Angriff genommen werden. Die Organisation muss nachweisen, dass sie Informationen oder Prozesse sauber prüft und letztendlich auch eine entsprechende Datenschutzfolgenabschätzung durchführen kann, um das Risiko für den Betroffenen im Falle einer Verletzung von Vertraulichkeit, Verfügbarkeit oder Integrität der Daten zu ermitteln.

Der nächste große Block ist die Sicherstellung von Reaktionsmechanismen auf Datenpannen. Hier geht es um die Beschreibung von Prozessen im Falle einer Meldung an die Aufsichtsbehörde. Auch diese Regelung ist mit dem §42a bereits im alten BDSG enthalten. Die DSGV hat dies neu aufgenommen. Letztlich muss hier ein sauberer Prozess mit Zuständigkeiten, Verantwortlichkeiten und Abläufen beschrieben werden. Das Gleiche gilt für die Organisation von Meldepflichten, also der Meldung an den Betroffenen, zu welchem Zweck welche Daten über ihn erhoben, gespeichert und verarbeitet werden.

Ein weiterer Block widmet sich den Auftragsbearbeitungen, wie beispielsweise dem Einsatz von Dienstleistern, Support oder Cloud-Lösungen. Wir stellen häufig in der Zusammenarbeit mit den Vereinen fest, dass keinerlei Auftragsdatenverarbeitungsverträge nach

dem alten §11 vorliegen. Hier sind die Organisationen in höchster Handlungsnot, sich eine Übersicht zu verschaffen, wer überhaupt als Auftragsverarbeiter eingesetzt wird und diese mit den entsprechenden rechtlich korrekten Verträgen zu versorgen, um Datenzugriff, -zugang, -nutzung, -weitergabe und -verarbeitung rechtlich auf sichere Füße zu stellen.

Des Weiteren muss sich ein Verein/Verband mit einer umfangreichen Dokumentation auseinandersetzen. Prüfprozesse, Auditierung, Auditprozesse – all das muss sauber definiert und letztlich auch niedergeschrieben sein. Es genügt nicht, sich einmalig einen Prozess anzuschauen, sondern es müssen Verfahren im eigenen Verein/Verband wiederkehrend in den Blick genommen werden. Sofern sich Änderungen im Verfahrensablauf, im Bereich der technisch-organisatorischen Maßnahmen oder in den Rechtsgrundlagen ergeben haben, muss ggf. noch einmal eine Datenschutzfolgenabschätzung durchgeführt werden.

Abschließend gibt es den gesamten Bereich der IT-Sicherheit: Wie sind Zugangs- und Zugriffsberechtigungen sauber geregelt und wie kann ich im Falle eines Datenverlustes meine Systeme möglichst schnell wiederherstellen, um die Datenverfügbarkeit zu garantieren? Auch diesen Fragen muss sich ein Verein/Verband widmen.

Dies sind erst einmal die wichtigsten Punkte, die bis Mai 2018 umgesetzt werden müssen.

Die Vereine und Verbände, die datenschutzrechtlich ihre Basishausaufgaben gemacht haben, wird ein überschaubarer und auch zu bewältigender Aufwand bis Mai 2018 erwarten. Schlecht sind die Vereine und Verbände gestellt, die sich noch gar nicht mit Thema beschäftigt haben und jetzt in sehr kurzer Zeit vieles auf die Beine stellen müssen. Ich empfehle in diesem Fall jedoch, nicht in reinen Aktionismus zu verfallen, sondern besonnen vorzugehen und erst einmal eine Bestandsaufnahme zu machen: was haben wir bereits erfüllt und wo besteht Nachbesserungsbedarf?

Red.:
Haben Sie weitere Anregungen, Tipps und Anmerkungen, die sie den Vereinen und Verbänden mit auf den Weg geben möchten?

D. M. Mülot:
Ich kann den Vereinen und Verbänden, vor allem den Vorständen und Geschäftsführungen nur empfehlen, sich in geeigneter Weise über das Thema zu informieren, beispielsweise in der von der Führungs-Akademie angebotenen Veranstaltungen zum Datenschutz oder im Datenschutz-Portal, um überhaupt erst einmal die Haftungsrisiken zu erkennen und einen Maßnahmenplan mit an die Hand zu bekommen, wie man letztendlich auch in der relativ kurzen Zeit noch möglichst viel erledigen kann. Natürlich setzt das immer die Bereitschaft voraus, dass jemand auch etwas tun möchte. Es ist hier aber keine Frage, die natürlich immer wieder im Raum steht, ob dieser Aufwand gerechtfertigt ist oder nicht. Niemand, auch kein Gesetzgeber, erwartet von einem Verein oder Verband, dass er Klassenbester ist. Aber er muss seine Basishausaufgaben machen. Bei vielen Organisationen ist nach wie vor ein Informationsdefizit vorhanden und die zu erfüllenden Basishausaufgaben sind unklar. Hier empfehle ich dringend, sich an kompetenter Stelle kundig zu machen und zu erfahren, welche Prioritäten gesetzt werden müssen. Daraus kann dann ein Maßnahmenplan entwickelt werden, der sukzessive abgearbeitet wird.

Red.: Vielen Dank für das Interview, Herr Mülot.

AKTUELLE URTEILE

6 Urteil zur elterlichen Aufsicht, Kontrolle und Gefahren-Abwendung bei digitalen 'smarten' Medien … sowie zu klaren Absprachen und Vorgaben zur familiären Mediennutzung[2]

Quelle: *Arbeitsgericht Bad Hersfeld, Urteil vom 15.05.2017; AZ: F 120/17 EASO*
Fundort: *Hessenrecht: Landesrechtsprechungsdatenbank: Entscheidungen der hessischen Gerichte*

Leitsätze des Urteils

1. Überlassen Eltern ihrem minderjährigen Kind ein digitales 'smartes' Gerät (z.B. Smartphone) zur dauernden eigenen Nutzung, so stehen sie in der Pflicht, die Nutzung dieses Geräts durch das Kind bis zu dessen Volljährigkeit ordentlich zu begleiten und zu beaufsichtigen.

2. Verfügen die Eltern selbst bislang nicht über hinreichende Kenntnisse von 'smarter' Technik und über die Welt der digitalen Medien, so haben sie sich die erforderlichen Kenntnisse unmittelbar und kontinuierlich anzueignen, um ihre Pflicht zur Begleitung und Aufsicht durchgehend ordentlich erfüllen zu können.

3. Es bestehen keine vernünftigen Gründe, einem Kind ein Smartphone auch noch während der vorgesehenen Schlafenszeit zu überlassen.

4. Zur Notwendigkeit einer Eltern-Kind-Medien-Nutzungsvereinbarung bei erheblichem Fehlverhalten in der Medien-Nutzung durch das Kind als auch durch ein Elternteil sowie aufkommender Medien-Sucht-Gefahr

5. Wer den Messenger-Dienst "WhatsApp" nutzt, übermittelt nach den technischen Vorgaben des Dienstes fortlaufend Daten in Klardaten-Form von allen in dem eigenen Smartphone-Adressbuch eingetragenen Kontaktpersonen an das hinter dem Dienst stehende Unternehmen.

   Wer durch seine Nutzung von "WhatsApp" diese andauernde Datenweitergabe zulässt, ohne zuvor von seinen Kontaktpersonen aus dem eigenen Telefon-Adressbuch hierfür jeweils eine Erlaubnis eingeholt zu haben, begeht gegenüber diesen Personen eine deliktische Handlung und begibt sich in die Gefahr, von den betroffenen Personen kostenpflichtig abgemahnt zu werden.

6. Nutzen Kinder oder Jugendliche unter 18 Jahren den Messenger-Dienst "WhatsApp", trifft die Eltern als Sorgeberechtigte die Pflicht, ihr Kind auch im Hinblick auf diese Gefahr bei der Nutzung des Messenger-Dienstes aufzuklären und die erforderlichen Schutzmaßnahmen im Sinne ihres Kindes zu treffen.

Im weitergehenden Text werden die aus den Leitsätzen abgeleiteten konkreten Entscheidungen des anhängigen Falles vorgestellt. [LINK zum vollständigen Text]

2 .

Vorherige Entscheidungen

Vgl. auch das erste Urteil des Amtsgerichts Bad Hersfeld zur „Pflicht zur elterlichen Aufsicht, Kontrolle und Gefahren-Abwendung bei digitalen 'smarten' Medien" vom 20.03.2017 (AZ: F 111/17 EASO).

Bereits in diesem Urteil hatte das Amtsgericht in einem familiengerichtlichen Beschluss die Mutter des Kindes u.a. dazu verpflichtet,

> „von allen Personen, welche aktuell im Adressbuch des Smartphones ihres Sohnes gespeichert sind, schriftliche Zustimmungserklärungen dahingehend einzuholen, ob diese Personen damit einverstanden sind,
>
> - dass ihr Sohn in dem Adressbuch seines Smartphones die Telefonnummer 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 ihrem Sohn gleichzeitig genutzte Applikation "WhatsApp" an den Betreiber WhatsApp Inc. in Kalifornien/USA übertragen / hochgeladen werden, wo diese Daten zu vielfältigen Zwecken des Betreibers laut dessen Nutzungsbedingungen frei weiter verwendet werden können. [LINK zum vollständigen Artikel]

Was bedeutet das Urteil für private WhatsApp Nutzer/-innen?

Unter dem Titel „Wider den ständigen Abmahnwahn – Warum KEIN gesteigertes Abmahnrisiko privater Whatsappnutzer besteht" setzt sich der Rechtsanwalt Dr. Carsten Ulbricht in seinem Rechtsblog mit den möglichen Konsequenzen dieses Urteils für private WhatsApp Nutzer/-innen auseinander.

Er wendet sich zunächst gegen die aus seiner Sicht überzogenen Warnungen in diversen Internetforen, die durch das Urteil eine Abmahnwelle auf alle WhatsApp Nutzer/innen zukommen sehen und vermutet dahinter in erster Linie das Bemühen der Herausgeber oder Betreiber dieser Foren, die eigenen Clickzahlen zu erhöhen.

Inhaltlich prognostiziert der Autor, dass das Urteil nicht zu einer massenhaften Zunahme von Abmahnverfahren gegen private WhatsApp Nutzer/innen führen werde. Dies nicht, weil kein datenschutzrechtlicher Verstoß vorliege, sondern vor allem auch, weil er die Haftung eher beim Anbieter und nicht beim Nutzer sieht.

„Bevor ich die Rechtslage, die man unter Zugrundelegung gewichtiger Stimmen in der Literatur und Rechtsprechung, durchaus anders sehen kann (vielleicht sogar muss) als das AG Bad Hersfeld, wage ich zu prognostizieren, dass das Internet wieder nicht untergehen wird und auch keine massenweisen Abmahnungen ausgesprochen werden."

Und weiter:

> *„Zunächst sind die Ausführungen des AG Bad Hersfeld zu der Weitergabe einzelner Kontaktdaten an den Betreiber wohl richtig. Zumindest bei der ersten Nutzung liest Whatsapp die Kontaktdaten aus, um festzustellen, ob bekannte Nutzer bereits Whatsapp nutzen.*

Diese Verfahren von Whatsapp kann man mit guten Argumenten kritisieren. Es lässt sich auch gut vertreten, dass Whatsapp mit dieser Datenverarbeitung jedenfalls bezüglich der betroffenen Kontakte gegen nationales und europäisches Datenschutzrecht verstößt, die Whatsapp nicht nutzen, demgemäß also auch in eine Nutzung seitens Whatsapp keinesfalls eingewilligt haben.

So sehr man Whatsapp für diese Datenverarbeitung kritisieren und vielleicht auch rechtlich gegen den Betreiber vorgehen kann, so sehr muss man diskutieren, ob hierfür tatsächlich auch die Nutzer rechtlich in Anspruch genommen werden können sollen. [LINK zum vollständigen Artikel]

Vgl. auch den Beitrag von C. Conrad, Justiziar des datenschutz nord, Bremen: „Datenschutz? Abmahngefahr?! – Was wir aus der WhatsApp-Entscheidung lernen können". In: „datenschutz notizen vom 11.07.17 [LINK zum Beitrag] [TN]

7 Anzeige urheberrechtlich geschützter Bilder in Suchmaschinen verletzt keine Urheberrechte

BGH verneint Urheberrechtsverletzung bei der Bildersuche durch Suchmaschinen

Quelle: *Bundesgerichtshof, Urteil vom 21.09.2017; AZ: - I ZR 11/16 -*
Fundort: *www. kostenlose-urteile.de (ra-online GmbH), Berlin 21.09.17; Dok.-Nr.: 24879*

Worum geht es?

Der Bundesgerichtshof hat entschieden, dass eine Anzeige von urheberrechtlich geschützten Bildern, die von Suchmaschinen im Internet aufgefunden worden sind, grundsätzlich keine Urheberrechte verletzt. Klägerin rügt Verletzung urheberrechtlicher Nutzungsrechte durch die Veröffentlichung von Vorschaubildern bei der Google-Bildersuche.

Die Klägerin des zugrunde liegenden Verfahrens betreibt eine Internetseite, auf der sie Fotografien anbietet. Bestimmte Inhalte ihres Internetauftritts können nur von registrierten Kunden gegen Zahlung eines Entgelts und nach Eingabe eines Passworts genutzt werden. Die Kunden dürfen die im passwortgeschützten Bereich eingestellten Fotografien auf ihre Rechner herunterladen.

Die Beklagte bietet auf ihrer Internetseite die kostenfreie Durchführung einer Bilderrecherche anhand von Suchbegriffen an, die Nutzer in eine Suchmaske eingeben können. Für die Durchführung der Bilderrecherche greift die Beklagte auf die Suchmaschine von Google zurück, zu der sie auf ihrer Webseite einen Link gesetzt hat. Die Suchmaschine ermittelt die im Internet vorhandenen Bilddateien, indem sie die frei zugänglichen Webseiten in regelmäßigen Abständen nach dort eingestellten Bildern durchsucht. Die aufgefundenen Bilder werden in einem automatisierten Verfahren nach Suchbegriffen indexiert und als verkleinerte Vorschaubilder auf den Servern von Google gespeichert. Geben die Internetnutzer in die Suchmaske der Beklagten einen Suchbegriff ein, werden die von Google dazu vorgehaltenen Vorschaubilder abgerufen und auf der Internetseite der Beklagten in Ergebnislisten angezeigt.

Klägerin rügt Verletzung urheberrechtlicher Nutzungsrechte durch Veröffentlichung von Vorschaubildern bei der Google-Bildersuche

Bei Eingabe bestimmter Namen in die Suchmaske der Beklagten wurden im Juni 2009 verkleinerte Fotografien von unter diesen Namen auftretenden Models als Vorschaubilder angezeigt. Die Bildersuchmaschine von Google hatte die Fotografien auf frei zugänglichen Internetseiten aufgefunden. Die Klägerin hat behauptet, sie habe die ausschließlichen Nutzungsrechte an den Fotografien erworben und diese in den passwortgeschützten Bereich ihrer Internetseite eingestellt. Von dort hätten Kunden die Bilder heruntergeladen und unerlaubt auf den von der Suchmaschine erfassten Internetseiten veröffentlicht. Sie sieht in der Anzeige der Vorschaubilder auf der Internetseite der Beklagten eine Verletzung ihrer urheberrechtlichen Nutzungsrechte und hat diese auf Unterlassung, Auskunftserteilung und Schadensersatz in Anspruch genommen.

BGH verneint Verletzung des ausschließlichen Rechts der Klägerin zur öffentlichen Wiedergabe der Lichtbilder

Das Landgericht Hamburg wies die Klage ab. Die Berufung der Klägerin blieb ohne Erfolg. Der Bundesgerichtshof wies die Revision der Klägerin zurück. Die Beklagte hat dadurch, dass sie die von der Suchmaschine aufgefundenen und als Vorschaubilder gespeicherten Fotografien auf ihrer Internetseite angezeigt hat, nicht das ausschließliche Recht der Klägerin aus § 15 Abs. 2 UrhG* zur öffentlichen Wiedergabe der Lichtbilder verletzt. Das gilt auch für den Fall, dass die Fotografien ohne Zustimmung der Klägerin ins frei zugängliche Internet gelangt sind. [LINK zum vollständigen Artikel]

8 Videoüberwachung in den Stadtbahnen und Bussen mit Datenschutzrecht vereinbar

Videoüberwachung dient der Wahrnehmung berechtigter Interessen der Verkehrsbetriebe

Quelle: *Niedersächsisches Oberverwaltungsgericht, Urteil vom 07.09.2017; AZ: 11 LC 59/16*
Fundort: *www. kostenlose-urteile.de (ra-online GmbH), Berlin 08.09.17; Dok.-Nr.: 24818*

Worum geht es?

Das Niedersächsische Oberverwaltungs-gericht hat entschieden, dass die Videoüberwachung in den Stadtbahnen und Bussen der ÜSTRA (Hannoversche Verkehrsbetriebe AG) mit dem Datenschutzrecht vereinbar ist. Das Gericht wies damit die Berufung der Landesbeauftragten für den Datenschutz Niedersachsen gegen ein Urteil des Verwaltungsgerichts Hannover zurück und bestätigte im Ergebnis die Aufhebung einer datenschutzrechtlichen Anordnung.

Im zugrunde liegenden Streitfall hatte die klagende ÜSTRA Hannoversche Verkehrsbetriebe AG in zahlreichen ihrer Fahrzeuge feststehende Videokameras installiert, mit denen im sogenannte Blackbox-Verfahren durchgehend Bewegtbilder vom Fahrzeuginnenraum aufgezeichnet werden. Die Videosequenzen werden nach 24 Stunden wieder ge-

löscht. Die Aufzeichnung dient unter anderem zur Beweissicherung bei Vandalismusschäden und zur Verfolgung von Straftaten.

Landesdatenschutzbeauftragte verfügt Einstellung der Videoüberwachung

Die Landesdatenschutzbeauftragte gab der ÜSTRA im August 2014 mit einer auf § 38 Abs. 5 des Bundesdatenschutzgesetzes gestützten Verfügung auf, die Videoüberwachung in ihren Bussen und Stadtbahnen während des Einsatzes der Fahrzeuge im öffentlichen Personennahverkehr einzustellen und erst wieder aufzunehmen, nachdem sie entweder ein Konzept für einen nach Linien und Zeit differenzierten Einsatz der Videotechnik erarbeitet und umgesetzt hat oder anhand konkreter Anhaltspunkte darlegt, dass die Videoüberwachung zeitlich und örtlich unbeschränkt erforderlich ist.

Klage der ÜSTRA vor dem Verwaltungsgericht erfolgreich

Der hiergegen gerichteten Klage gab das Verwaltungsgericht Hannover mit der Begründung statt, dass das Bundesdatenschutzgesetz nicht anwendbar sei, weil die ÜSTRA eine öffentliche Stelle des Landes Niedersachsen sei, für die der Datenschutz durch Landesgesetz geregelt sei. Das niedersächsische Datenschutzgesetz enthalte keine Eingriffsermächtigung, auf die die Verfügung der Landesdatenschutzbeauftragten gestützt werden könnte. [LINK zum vollständigen Artikel]

Führungs-Akademie
des Deutschen Olympischen Sportbundes
Willy-Brandt-Platz 2
50679 Köln

Tel. 0221/221 220 13
Fax: 0221/221 220 14
info@fuehrungs-akademie.de
www.fuehrungs-akademie.de