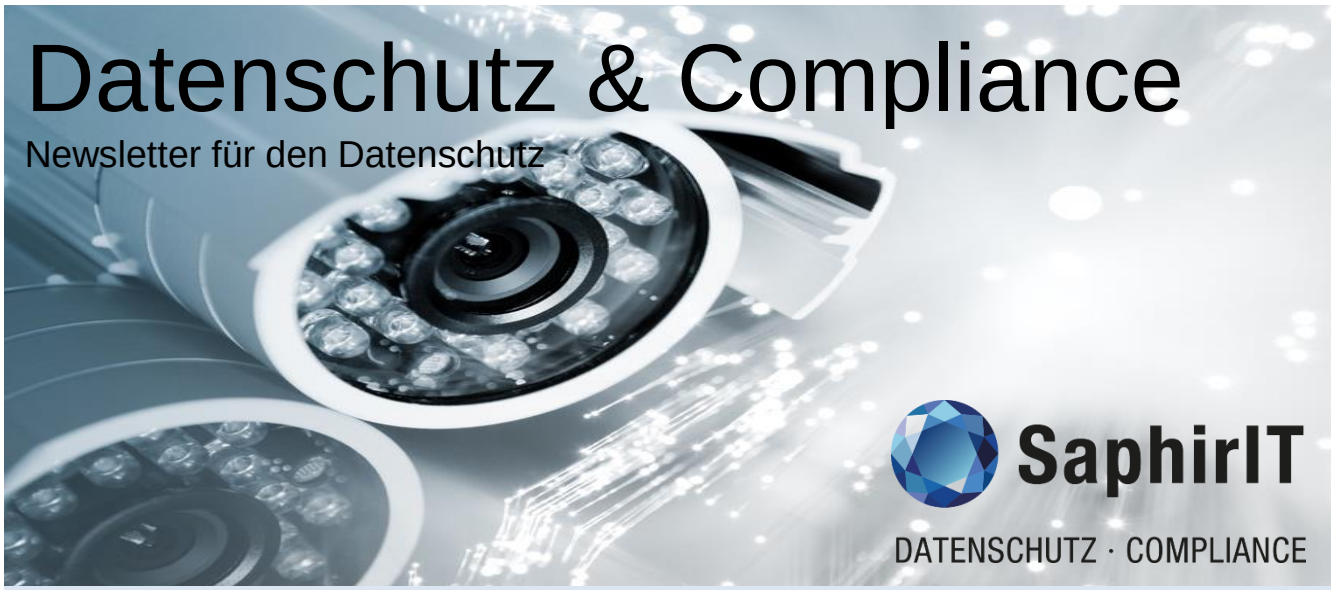

Ausgabe Mai 2018 | Seite 61 - 65

INHALT

Sehr geehrte Damen und Herren,

hiermit übersenden wir Ihnen unseren aktuellen Newsletter Mai 2018.

Heute, am **25.05.2018**, erlangt die Datenschutzgrundverordnung ihre Wirksamkeit. Spätestens zum heutigen Tage sollten Sie in Ihrem Unternehmen die wichtigsten Prozesse und Verfahren bereits an die Verordnung angepasst haben. Andernfalls drohen ab sofort enorme Bußgelder, Schadensersatz- und Schmerzensgeldansprüche, als auch das Risiko wegen eines Datenschutzverstoßes kostenpflichtig abgemahnt zu werden.

Wir wünschen Ihnen viel Spaß bei der Lektüre. Sollten Sie bei sich dennoch kurzfristig Handlungsbedarf sehen, setzen Sie sich gerne mit uns in Verbindung (www.saphirit.de).

Mit freundlichen Grüßen
Ihre SaphirIT GmbH

E-Mail Werbung nach der DSGVO:

Problematik des Re-Opt-In-Verfahrens

- Anforderungen an eine Einwilligung nach der Datenschutzgrundverordnung (DSGVO) -

Viele Unternehmen nutzen mittlerweile den E-Mail Versand, um ihren Kunden oder auch potentiellen Kunden Newsletter oder auch Werbung zusenden zu können.

Im Hinblick auf die nun geltende Datenschutzgrundverordnung ist allerdings Vorsicht geboten. Vor allem bedarf es einer ausdrücklichen Einwilligung jedes Newsletter Abonnenten, die

im Zweifel auch nachgewiesen werden können muss.

Bereits nach jetziger Rechtslage ist es nötig, dass Unternehmen eine ausdrückliche Einwilligung einholen. Auch nach der neuen Rechtslage muss hieran festgehalten werden. Insbesondere im Hinblick auf die umfassende Nachweis- und Rechenschaftspflicht sollten Unternehmen im Zweifel auch in der Lage sein nachzuweisen, dass eine solche Einwilligung vorliegt.

Problematisch stellt sich der Versand jetzt aber vor allem im Hinblick auf Alt-Einwilligungen dar. Sind bestehende Einwilligungen ausreichend? Müssen diese Einwilligungen neu eingeholt werden? Und wie sieht es mit der Möglichkeit eines Re-Opt In Verfahrens aus. Alles Fragen, die im Hinblick auf die Datenschutzgrundverordnung nun geklärt werden müssen.

Um massenhafter E-Mail-Werbung entgegenzuwirken regelt das Gesetz gegen den unlauteren Wettbewerb (UWG) dass, vor dem erstmaligen Versand einer E-Mail eine Einwilligung eingeholt werden muss.

Die Frage wie lange eine einmal eingeholte Einwilligung Wirksamkeit entfaltet, wurde in der Vergangenheit von vielen Gerichten unterschiedlich entschieden. So sah das AG Hamburg keinen zeitlichen Ablauf von Einwilligungserklärungen. Das LG Stuttgart, das LG München, das LG Berlin oder das AG Bonn dagegen sahen einen automatischen Ablauf der Einwilligungserklärung nach 4 Wochen, 1,5 Jahren, 2 Jahren, oder nach bis zu 4 Jahren.
Mit Urteil vom 01.02.2018 hat der Bundesgerichtshof (BGH) für klare Verhältnisse gesorgt. „Eine zeitliche Begrenzung einer einmal erteilten Einwilligung sieht weder die Richtlinie 2002/58/EG noch § 7 UWG vor. Hieraus ergibt sich, dass diese – ebenso wie eine Einwilligung nach § 183 BGB – grundsätzlich nicht allein durch Zeitablauf erlischt.“

Da der BGH aber auch in diesem Fall, wie häufig, nur „grundsätzlich“ kein automatisches Erlöschen der Einwilligungserklärung sieht, bleibt abzuwarten, ob dieser Grundsatz im Einzelfall nicht durchaus doch anders bewertet werden wird.

Somit kann erst einmal davon ausgegangen werden, dass eine Person, die einmal wirksam ihre Einwilligung erteilt hat, unbegrenzt E-Mails zugesandt bekommen darf. Natürlich nur soweit diese Einwilligung nicht widerrufen wurde.

Auch für Kontakte die mündlich in den Versand eingewilligt haben, oder dies durch Überreichen ihrer Karte gemacht, bedarf es grundsätzlich einer „ausdrücklichen“ Einwilligung. Dadurch, dass die Datenschutzgrundverordnung eine Rechenschaftspflicht der Unternehmen annimmt, muss dieses im Zweifel nachweisen können, dass der Betroffene eingewilligt hat, was bei mündlichen Erklärungen nur schwer möglich sein dürfte.

Viele Unternehmen bedienen sich deshalb der sogenannten Re-Opt-In Möglichkeit. Hier sollen alle E-Mail Empfänger per Mail erneut aufgefordert werden ihre Einwilligung zu erteilen.

Wenn man allerdings davon ausgeht, dass die vorher erteilte Einwilligung nicht wirksam war, dann aber per E-Mail darum gebeten wird die Einwilligung nachzuholen, wäre bereits diese Kontaktaufnahme als Werbung zu sehen, für die keine Grundlage besteht. Mithin wäre im Grunde dem Problem auch hiermit nicht ausreichend Rechnung getragen.

Auch wenn es somit nach momentaner Rechtslage keine „saubere Lösung“ gibt, um „defekte Einwilligungen“ zu reparieren, sollte speziell im Hinblick auf die Nachweispflicht, von allen Empfängern, soweit noch nicht vorhanden, eine ausdrückliche Einwilligung eingeholt werden.

Bei neuen E-Mail-Adressen die in einen Verteiler aufgenommen werden, sollte dann direkt darauf geachtet werden eine wirksame Einwilligung einzuholen. Bereits wirksam eingeholte Einwilligungen müssen nach Erwägungsgrund 171 der Datenschutzgrundverordnung nicht erneut eingeholt werden.

Nach Gesichtserkennung nun auch Verhaltenserkennung am Berliner Bahnhof Südkreuz

- Projekt Südkreuz geht in die zweite Runde -

Im August vergangenen Jahres startete in Berlin das Experiment „Gesichtserkennung“. 300 Freiwillige wurden mit ihren biometrischen Daten in eine Datenbank eingespeist. Die Bundespolizei speicherte diese Fotos der Freiwilligen ab und gleicht diese mit allen Gesichtern ab, die sie in dem markierten Bereich des Bahnhofs durch die installierten Kameras erfasst.

Anders als in dieser Testphase sollen bei einem möglicherweise realen Betrieb keine freiwilligen Gesichtsdaten, sondern Personen aus Fahndungsdatenbanken erkannt werden.

Auch wenn der ehemalige Innenminister Thomas de Maizière das Experiment bereits jetzt als Erfolg ansieht und die Testphase im Dezember um weitere 6 Monate verlängerte dürfen auch die Risiken und negativen Aspekte nicht außer Acht gelassen werden.

70 % der Gesuchten Personen seien richtig erkannt worden. Unter ein Prozent der erfassten Personen seien irrtümlich als einer der Freiwilligen identifiziert worden. Hört sich erst einmal nicht nach viel an. Rechnet man dies allerdings einmal auf die täglich am Berliner Südkreuz passierenden 100.000 Reisenden hoch, so ergeben sich 1.000 falsche Verdächtige.

Vor allem das Tragen von Schals und Mützen erschwere die fehlerfreie Identifikation.

Nicht nur, dass jede von den Kameras erfasste Person mithin als möglicher Täter aus dem Verkehr gezogen werden kann, die Gesichtserkennung schränkt jeden, der von den Kameras aufgenommen wird massiv in seinem Persönlichkeitsrecht ein.
Die Tatsache, dass jetzt auch das Verhalten aller Personen analysiert werden soll führt dazu, dass man bei jeder Bewegung damit rechnen muss sich in irgendeiner Weise auffällig zu verhalten, auch wenn man möglicherweise nur nervös den Bahnsteig auf und ab läuft, weil die Bahn wieder einmal zu spät kommt.

Es wird abzuwarten bleiben ob und inwieweit das Experiment in Zukunft tatsächlich real umgesetzt wird.

Alternative Messenger: Problematik bei der Verwendung von WhatsApp nach der DSGVO

WhatsApp hat 1,5 Milliarden Nutzer weltweit. Auch viele Unternehmen nutzen den beliebtesten Messaging-Dienst,. sei es zur internen Mitarbeiterkommunikation oder zur Kundenbetreuung.

Das Problem, dass sich im Hinblick auf die DSGVO ergibt lässt sich relativ schnell zusammenfassen. WhatsApp überträgt das Telefonbuch seiner Nutzer auf die firmeneigenen Server in den USA. Darunter nicht nur die Kontakte derer, die WhatsApp Nutzer sind, sondern alle Kontakte die im Smartphone abgespeichert sind.

Grundsätzlich verboten ist das Übertragen von Daten in ein Drittland außerhalb der EU nicht. Am sichersten wäre eine sogenannte Opt-In Option. Das Einholen einer nachweisbaren Einwilligung jedes einzelnen Kontakts erscheint dabei aber kaum umsetzbar.

Liegt eine solche Einwilligung also nicht vor, kann die Datenübertragung nur erfolgen, wenn sie entweder zur Vertragserfüllung notwendig ist oder die Interessen des Unternehmens die Interessen der Betroffenen überwiegen. Da dies in den allermeisten Fällen nicht der Fall ist, ist eine datenschutzkonforme Nutzung von WhatsApp zu Unternehmenszwecken nicht gegeben.

Neben der fehlenden Datenübertragungsbefugnis bietet WhatsApp seinen Nutzern zudem nicht die Möglichkeit der Löschung der eigenen Daten, worauf jeder Nutzer nach der Datenschutzgrundverordnung allerdings einen Anspruch hat.

Auch wenn es zur Problematik rund um WhatsApp nach der DSGVO noch keine Rechtsprechung gibt, kann Unternehmen nur dringend geraten werden ab dem heutigen Tage auf die dienstliche Nutzung von WhatsApp zu verzichten.

Wer dennoch nicht auf die Verwendung eines Messengers verzichten kann oder will, sollte sich einmal mit den datenschutzkonformen Alternativen auseinandersetzen.

„Grape“, „Threema“ oder der Messenger „Signal“ übertragen das Adressbuch ihrer Nutzer nicht. Zudem stehen die Server dieser Dienstleister in der EU oder in einem anderen Drittland, welches aber anders als die Vereinigten Staaten über ein angemessenes Datenschutzniveau verfügt.

Entgegen der Vermutung vieler stellt auch der Dienst „Telegram“ keine datenschutzkonforme Alternative zu WhatsApp dar. Zwar stehen die zumindest bekannten Server in London, dennoch ist nicht transparent in welchen Rechenzentren welche Daten wie verarbeitet werden. Telegram bedient sich zudem des gleichen Verfahrens zum Abgleich des Adressbuchs wie WhatsApp.

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