Geschäftsstelle Dresden:
Königsbrücker Landstraße 40
01109 Dresden
Tel: 0351 8881251

Niederlassung Böblingen:
Otto-Lilienthal-Straße 36
71034 Böblingen
Tel: 07031 7145660

mail@sodalitas-gmbh.de
www.sodalitas-gmbh.de
Fax: 0351 8881252

IT-Ticker 03/2019

Der IT-Ticker 03/2019 informiert Sie über folgende Themen:

EuGH: Anforderungen an eine Cookie-Einwilligung

Der EuGH hat am 01.10.2019 entschieden, dass Betreiber von Webseiten eine Einwilligung in das Setzen von Cookies für Werbezwecke nicht durch ein vorangekreuztes Häkchen einholen können (Urteil v. 01.10.2019, Az. C-673/17).

Vielmehr müsse der Nutzer aktiv ein Häkchen setzten, um seine Einwilligung zu erteilen. Die Entscheidung des EuGH gilt unabhängig davon, ob die in dem Cookie gespeicherten Daten personenbezogene Daten darstellen oder nicht. Weitere Voraussetzung für eine wirksame Einwilligung ist nach dem Urteil, dass der Nutzer über die Funktionsdauer des Cookies und mögliche Zugriffsrechte Dritter auf den Cookie informiert wurde.

Hintergrund des Verfahrens ist ein deutscher Rechtsstreit. Der Verbraucherzentrale Bundesverband hatte einen Gewinnspielanbieter auf Unterlassung in Anspruch genommen, weil im Rahmen einer Gewinnspielteilnahme die Einwilligung in das Setzen von Cookies durch ein vorangekreuztes Häkchen eingeholt werden sollte. Mit dem Cookie wurde das Nutzungsverhalten der Teilnehmer über mehrere Webseiten getrackt. Die Ausführungen des EuGH gehen dabei jedoch nicht auf besondere Anforderungen von Cookies ein, sondern befassen sich allgemein mit der Einwilligung. Sie sind daher auch anwendbar auf die (noch) weit verbreiteten Cookie-Banner, mit denen Seitenbetreiber über den Einsatz von Cookies informieren und lediglich eine Möglichkeit zum Opt-out einräumen („Durch die weitere Nutzung unserer Seite stimmen Sie der Verwendung von Cookies zu.“).

Der EuGH hat sich in der Entscheidung nicht mit der Frage befasst, in welchen Fällen eine Einwilligung in das Setzen eines Cookies erforderlich ist. Er hat aber konkrete Vorgaben dafür formuliert, wie eine Einwilligung einzuholen ist. Die Entscheidung hat daher keinen Einfluss auf Cookies, die für die Funktionsfähigkeit einer Webseite zwingend erforderlich sind (Login-Sessions, Warenkorb, Spracheinstellungen).

Die Datenschutzkonferenz („DSK“) hatte im März 2019 eine Orientierungshilfe für Anbieter von Telemedien veröffentlich, in der Sie ihre Position zu Cookies noch einmal dargelegt hat. Nach der Auffassung der DSK können Cookies, die das Nutzerverhalten über verschiedene Webseiten tracken nicht auf Grundlage des berechtigten Interesses der Seitenbetreiber eingesetzt werden, sondern nur über eine ausdrückliche Einwilligung.

Praxis-Tipp: Seitenbetreiber sollten prüfen, ob und welche Cookies auf der Seite eingesetzt werden. Einwilligungen müssen an die Anforderungen des EuGH angepasst werden. Danach müssen Cookies, für die eine Einwilligung eingeholt werden soll, vor der ausdrücklichen Einwilligung inaktiv sein. In den Datenschutzhinweisen muss die Speicherdauer von Cookies angegeben werden und es bedarf einer Klarstellung, ob Dritte Zugriff auf die Cookies haben.

Nikolaus Bertermann, Berlin
n.bertermann@skwschwarz.de

Bußgeldmodell der Aufsichtsbehörden für Datenschutz

Bußgelder für Datenschutzverstöße werden sich voraussichtlich grundsätzlich erhöhen.

Weitgehend unbemerkt von der Öffentlichkeit hat die „Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder“ (DSK) bereits im Juni 2019 über ein neues Berechnungsmodell für Bußgelder diskutiert. Dieses soll ähnlich wie im Kartellrecht eine nachvollziehbare Bußgeldpraxis ermöglichen.

Zwar soll das Modell selbst – trotz expliziter Anfragen – derzeit nicht veröffentlicht werden. Eine Anwendung in der Praxis erfolgte jedoch bereits (allein zu Testzwecken wie die DSK betont). Ersten Berichten zur Folge wird das Bußgeldmodell sehr wahrscheinlich zu einer signifikanten Erhöhung der Bußgelder führen. Dieses darf angesichts der stark gestiegenen gesetzlichen Bußgeldandrohung von bis zu 4% des weltweit erzielten Vorjahresumsatzes oder € 20 Millionen nicht überraschen. Ein genauerer Blick auf die bisweilen verfügbaren Informationen lässt jedoch darauf schließen, dass Bußgelder wie die bereits verhängten € 110 Millionen gegen die Hotelkette Marriott oder die € 204 Millionen gegen die Fluglinie British Airways auch in Deutschland wahrscheinlicher werden.

Die Datenschutzkonferenz bestätigt in einer Pressemitteilung die Existenz eines entsprechenden Berechnungsmodells, gibt jedoch derzeit keine Details preis und verweist darauf, dass das Modell zur Prüfung der Praxistauglichkeit und Zielgenauigkeit in konkreten Bußgeldverfahren zunächst nur „getestet“ werde. Auf einer weiteren Konferenz im November werde hierüber weiter beraten. Dann soll auch über die Veröffentlichung des Konzepts entschieden werden.

Obwohl es noch nicht veröffentlicht ist, lässt sich das geplante Modell anhand der Begründung von bereits erlassenen Bußgeldbescheiden zumindest teilweise nachvollziehen. So werde für die Verhängung von Bußgeldern nach Art. 83 DSGVO zunächst ein wirtschaftlicher Grundwert in Form eines sogenannten „Tagesumsatzes“ berechnet. Im Anschluss solle mit Hilfe des Tagesumsatzes ein Regelbußgeldkorridor und ein Mittelwert errechnet werden. Hierzu werde zunächst der Verstoß als leicht, mittel, schwer oder sehr schwer kategorisiert. Welcher Verstoß welcher Kategorie entspreche, hänge von dessen Unrechtsgehalt ab. Auch der Verschuldensgrad des Verantwortlichen an dem Verstoß solle neben weiteren Aspekten berücksichtigt werden. Die Höhe des Bußgeldes ergibt sich anschließend aus der Multiplikation des Kategoriewertes mit dem Tagesumsatz.

Beispielsweise stelle die unverlangte Zusendung von Werbemails einen leichten Verstoß dar. Hat ein Unternehmen mit einem Jahresumsatz von € 36 Millionen mithin einen leichten Verstoß begangen, so ergibt sich hieraus zunächst ein Tagesumsatz in Höhe von € 100.000,00 (Jahresumsatz dividiert durch 360), der in der leichten Kategorie einen Regelbußgeldkorridor von € 100.000,00 bis zu € 400.000,00 (Kategoriewert 1 – 4) entspreche. Der diesbezügliche Mittelwert wäre dann € 250.000,00. Von diesem Mittelwert ausgehend wird das Bußgeld dann weiter nach oben oder unten verschoben. Ausschlaggebend sollen insbesondere die Dauer, Art, Umfang und Zweck, die Anzahl der betroffenen Personen, das Ausmaß des erlittenen Schadens sowie der Verschuldensgrad sein. Am Ende könne der Mittelwert um mehrere 100 Prozent ansteigen oder auch gesenkt werden.

Fraglich ist jedoch, ob das so geplante Bußgeldmodell tatsächlich auch den – von der DSGVO ebenfalls geforderten Grundsatz der Verhältnismäßigkeit – berücksichtigt. Verhältnismäßig bedeutet vor allem, dass Sanktionen tat- und schuldangemessen sein müssen. Diese Anforderung berücksichtigt das neue Bußgeldmodell nur teilweise, da es sich vorrangig am weltweiten Gesamtumsatz des Unternehmens orientiert. Dies bedeutet, dass umsatzstarke Unternehmen schon für einen relativ geringfügigen Verstoß ein hohes Bußgeld zu zahlen hätten. Zwar ist dies aufgrund der Abschreckungsfunktion eines Bußgeldes ansatzweise gewollt. Jedoch darf ein Bußgeld nicht allein aufgrund eines hohen Jahresumsatzes bereits im Mittelwert unverhältnismäßig zum begangenen Verstoß sein.

Folgen für die Praxis:
Auch wenn die bisweilen verfügbaren Informationen noch nicht offiziell bestätigt sind und auch nicht final zu sein scheinen, so lassen sie doch auf den Willen der Datenschutzaufsichtsbehörden schließen, das Spektrum möglicher Bußgelder auszunutzen. Die Berechnungsmethode führt auch bei mittelständischen Unternehmen bereits zu gravierenden Bußgeldrisiken, die sich scheinbar an den diesbezüglichen Maßstäben bei Kartellverstößen orientieren. Es sind berechtigte Zweifel angezeigt, ob eine solche Berechnung noch verhältnismäßig im Sinne des Art. 83 Abs. 1 DSGVO ist. In der Praxis relevant ist der Umstand, dass die Gerichte an entsprechende Leitlinien zur Bußgeldverhängung nicht gebunden sind, sondern ein eigenständiges volles Prüfrecht besitzen. Es steht somit zu erwarten, dass die Gerichte ebenfalls einen erheblichen Einfluss auf das Bußgeldmodell nehmen werden.

Franziska Ladiges, Frankfurt/Main
f.ladiges@skwschwarz.de
Dr. Hendrik Skistims, Frankfurt/Main
h.skistims@skwschwarz.de

EuGH: Bezahlung per Lastschrift darf nicht von Wohnsitz im Inland abhängig gemacht werden

Im Online-Handel werden den Kunden üblicherweise mehrere alternative Zahlungsmethoden (Rechnungskauf, Lastschrift, Kreditkarte, PayPal usw.) zur Verfügung gestellt. Allerdings bieten Händler die Nutzung bestimmter Zahlungsmethoden häufig nur ausgewählten Kundengruppen an bzw. stellen für die Nutzung besondere Anforderungen auf. So ist ein Rechnungskauf vielfach nur für solche Kunden möglich, die bereits zuvor bei dem jeweiligen Händler gekauft haben. Mit einer anderen Fallkonstellation musste sich der Europäische Gerichtshof in einer aktuellen Entscheidung (EuGH, Urt. v. 05.09.2019, Rechtssache C-28/18 – Verein für Konsumenteninformation / Deutsche Bahn AG) befassen:

In dem konkreten Fall hatte der österreichische Verein für Konsumenteninformation vor den österreichischen Gerichten eine Klausel in den Beförderungsbedingungen der Deutschen Bahn beanstandet, wonach eine über die Webseite der Deutschen Bahn getätigte Buchung nur dann per Lastschrift bezahlt werden kann, wenn der Kunde seinen Wohnsitz in Deutschland hat. Da die Beantwortung der Frage, ob eine solche Klausel zulässig ist, maßgeblich von der Auslegung europäischer Vorschriften abhängt, hatte der mit der Rechtssache befasste österreichische Oberste Gerichtshof diese Frage dem EuGH zur Vorabentscheidung vorgelegt.

Nach Auffassung des EuGH verstößt die Klausel in den Beförderungsbedingungen der Deutschen Bahn tatsächlich gegen europäisches Recht, nämlich die Verordnung (EU) Nr. 260/2012 zur Festlegung der technischen Vorschriften und der Geschäftsanforderungen für Überweisungen und Lastschriften in Euro: Denn nach dieser Verordnung solle es Verbrauchern ermöglicht werden, für jegliche Zahlung innerhalb der Europäischen Union per Lastschrift nur ein einziges Zahlungskonto zu nutzen, um damit Kosten, die mit der Führung mehrerer Zahlungskonten verbunden sind, zu vermeiden. Mit der streitgegenständlichen Klausel werde jedoch gerade indirekt der EU-Mitgliedsstaat bestimmt, in dem das Zahlungskonto geführt werden muss.

Die Unzulässigkeit der Klausel besteht nach Auffassung des EuGH abhängig davon, ob der Händler alternative Zahlungsmethoden anbieten würde. Zwar könne der Händler frei entscheiden, ob er die Zahlungsmethode „Lastschrift“ anbiete. Bietet er sie an, dürfe er dem Kunden jedoch nicht indirekt vorschreiben, in welchem EU-Mitgliedstaat das Zahlungskonto zu führen sei. Das Missbrauchs- oder Zahlungsausfallrisiko könne der Händler zudem dadurch verringern, dass er die Fahrkarten erst dann liefert bzw. deren Ausdruck ermöglicht, nachdem der erfolgreiche Einzug der Zahlung bestätigt wurde.

Praxistipp:
Händler, die die Zahlungsmethode „Lastschrift“ anbieten, sollten – unabhängig davon, ob weitere Zahlungsmethoden gewählt werden können – die Auswahl dieser Zahlungsmethode nicht länger von einem Wohnsitz des Kunden im Inland abhängen machen. Dies betrifft sowohl technische Beschränkungen als auch Beschränkungen in Allgemeinen Geschäftsbedingungen.

Jens Borchardt, Hamburg
j.borchardt@skwschwarz.de

Neues aus dem E-Commerce: PSD2 & Starke Kundenauthentifizierung (SCA)

Der 14.9. ist ein weiterer Meilenstein für die PSD2: Spätestens ab dem 14. September 2019 sollten Zahlungsdienstleister in der EU eine sog. „Starke Kundenauthentifizierung“ (SCA) durchführen müssen, wenn der Zahler einen elektronischen Zahlungsvorgang auslöst.

Beim neuen Begriff der „Starken Kundenauthentifizierung“ werden zur Identifikation des Zahlenden zwei voneinander unabhängige Elemente verwendet. Die Elemente müssen aus zwei der drei Kategorien

- Wissen,
- Besitz und
- Inhärenz

stammen. Beispiele dafür sind ein Passwort (Wissen), ein Mobiltelefon (Besitz) oder ein persönlicher Fingerabdruck (Inhärenz).

Die neuen Vorgaben zur SCA sollen nun auch für Kreditkartenzahlungen im Internet verwendet werden. Die bislang übliche Authentifizierung über die Eingabe von Kreditkartennummer und Prüfziffer erfüllt die neuen Vorgaben nicht. Vielmehr sind auch hier zusätzlich zwei Elemente aus den erwähnten Kategorien zu verwenden. Ausnahmen von den neuen Anforderungen sind eng begrenzt und betreffen beispielsweise bestimmte Kleinbetragszahlungen.

Allerdings hat die Bafin schon verlauten lassen, dass sie die SCA für Kreditkartenzahlungen erst einmal verschiebt (siehe Pressemitteilung vom 21. August). Zahlungsdienstleister haben daher zunächst Entscheidungszeit gewonnen, um sich auf die Umsetzung der neuen PSD2-Vorgaben in Deutschland vorzubereiten. Es gilt dann aber genau zu beobachten, wie sich die BaFin in ihrer Position weiter entwickelt.

Praxistipp:
Von den SCA-Vorgaben sind in erster Linie Zahlungsdienstleister betroffen. Andere E-Commerce-Akteure, wie beispielsweise Online-Shops, sollten jedoch bei ihren Zahlungsdienstleistern in Erfahrung bringen, ob die SCA-Vorgaben eingehalten werden.

Dr. Tatjana Schroeder, Frankfurt/Main
t.schroeder@skwschwarz.de
Yvonne Schäfer, Frankfurt/Main
y.schaefer@skwschwarz.de

Ist mein Unternehmen DSGVO konform?

Die DSGVO gilt seit mehr als einem Jahr. Die meisten Unternehmen haben viel Zeit und Geld aufgewendet, um die neuen datenschutzrechtlichen Anforderungen umzusetzen.

Nachdem nun die Umsetzungshektik verflogen ist, sollte man sich die Zeit nehmen und das Geschaffene einer kritischen Prüfung unterziehen. Nur so wird man nicht überrascht, wenn sich ein Betroffener beschwert oder gar die Aufsichtsbehörde prüft.

Sehr hilfreich ist, dass die Aufsichtsbehörden die Fragen veröffentlicht haben, die sie im Zusammenhang mit ihren ersten Prüfungen stellen. So hat der Landesbeauftragte für den Datenschutz Niedersachsen den „Kriterienkatalog zur Querschnittsprüfung in der Wirtschaft 2018/19“ veröffentlicht (https://lfd.niedersachsen.de/startseite/datenschutzreform/ds_gvo/kriterien-querschnittspruefung-179455.html). Darin sind nicht nur Standardfragen zum Verzeichnis der Verarbeitungstätigkeiten oder zu den Betroffenenrechten enthalten. Die Fragen gehen in ihren ca. 200 Einzelkriterien auch in die Tiefe. Gefragt wird z. B. nach den Voraussetzungen für die Datenlöschung.

Beim technischen Datenschutz werden der risikobasierte Ansatz und der damit zusammenhängende Abwägungsprozess untersucht. Bei der Datenschutzfolgenabschätzung werden nicht nur die vorhandenen Datenschutzfolgenabschätzungen geprüft. Die Untersuchung setzt bereits eine Stufe früher ein und prüft den Entscheidungsprozess, ob bei Verarbeitungen eine

Datenschutzfolgenabschätzung durchgeführt werden muss oder nicht. Hinzu kommen viele weitere Detailfragen.

Auch das bayerische Landesamt für Datenschutzaufsicht hat bereits mit der Prüfung der Umsetzung der DSGVO bei kleinen und mittelständischen Unternehmen begonnen. Ein entsprechender Fragenkatalog wurde ebenfalls veröffentlicht (https://www.lda.bayern.de/media/pruefungen/201811_kmu_fragebogen.pdf).

Praxistipp:
Prüfen Sie die Umsetzung der DSGVO in Ihrem Unternehmen anhand der veröffentlichten Fragenkataloge. Gerne unterstützen wir Sie mit der fachkundigen Analyse der vorhandenen Abläufe und Dokumentationen.

Dr. Oliver M. Bühr, Frankfurt/Main
o.buehr@skwschwarz.de

OLG Frankfurt a. M.: Teilnahme an einem Gewinnspiel kann von der Einwilligung in den Erhalt künftiger Werbung abhängig gemacht werden

Das OLG Frankfurt a. M. hat mit Urteil vom 27.06.2019, Az. 6 U 6/19, zu verschiedenen wettbewerbsrechtlichen und datenschutzrechtlichen Aspekten bei dem Zusammenspiel eines Einwilligungserfordernisses und der Teilnahme an einem Gewinnspiel Stellung genommen.

Dabei hat das OLG Frankfurt a. M. entschieden, dass die Teilnahme an einem Gewinnspiel von der Einwilligung in den Erhalt künftiger Werbung abhängig gemacht werden kann. Im amtlichen Leitsatz ist nur von E-Mail-Werbung die Rede. In den Entscheidungsgründen geht es insbesondere um die Einwilligung in Werbeanrufe, die offenbar allein klagegegenständlich waren. Nachdem bei Vorliegen einer ordnungsgemäßen Einwilligung gesetzlich beides möglich ist, ist dieser Umstand nicht von entscheidender Bedeutung (vgl. § 7 Abs. 2 Nr. 2 und Nr. 3 UWG).

Zudem hat das OLG Frankfurt a. M. entschieden, dass die Einwilligung zugunsten mehrere werbetreibender Unternehmen („Werbetreibende“) eingeholt werden kann. Dabei sind Werbemedium und insbesondere das Produkt- oder Leistungsangebot der einzelnen Werbetreibenden hinreichend klar zu bezeichnen. Wenn die Werbemaßnahmen eines Werbetreibenden nicht hinreichend bezeichnet sind, ändert dies grundsätzlich nichts an der Wirksamkeit der Einwilligung gegenüber den anderen Werbetreibenden.

Einwilligungserfordernis und Gewinnspielteilnahme

Die Datenschutz-Grundverordnung („DSGVO“) regelt, dass eine Einwilligung u.a. freiwillig erfolgen muss. Im Rahmen der Prüfung dieser Freiwilligkeit ist auch zu untersuchen, ob die Erfüllung eines Vertrages von der Einwilligungserteilung abhängig gemacht wird (vgl. Art. 7 Abs. 4 DSGVO, sog. allgemeines Kopplungsverbot). Die deutschen Datenschutzaufsichtsbehörden vertreten hierbei, soweit ersichtlich, eine relativ strikte Ansicht. Danach sollte eine betroffene Person grundsätzlich die Möglichkeit haben, einen Vertrag (über die Gewinnspielteilnahme) abzuschließen, ohne eine (Werbe-)Einwilligung erteilen zu müssen. Etwas anders könne gelten, wenn die datenschutzrechtliche Einwilligung zwingend erforderlich ist, um das Vertragsziel zu erreichen. Dies sind aber spezielle Fälle bei der Verarbeitung von besonderen Kategorien personenbezogener Daten.

Übertragen auf Gewinnspiele führte dies in der Praxis, seit DSGVO-Einführung, dazu, die Gewinnspielteilnahme unabhängig von dem Erfordernis einer Werbeeinwilligung auszugestalten.

Diese restriktive Ansicht müsste mit dem OLG Frankfurt a. M. nicht weiterverfolgt werden. Das OLG Frankfurt a. M. hat das Merkmal „freiwillig“ mit dem Begriff „ohne Zwang“ gleichgesetzt. Eine betroffene Person sei nicht gezwungen an einem Gewinnspiel teilzunehmen. Daraus folgt, dass sie auch nicht gezwungen ist, eine Werbeeinwilligung abzugeben. Die Verknüpfung eines Einwilligungserfordernisses mit der Teilnahme an einem Gewinnspiel stehe der Freiwilligkeit einer solchen Einwilligung nicht entgegen. Der Verbraucher könne und müsse selbst entscheiden, ob ihm die Teilnahme die Preisgabe seiner Daten „wert“ ist. Auf das sogenannte allgemeine Kopplungsverbot nimmt das OLG Frankfurt a. M. nach diesen Feststellungen keinen Bezug.

Einwilligung zugunsten mehrerer Werbetreibender

Eine Einwilligungserklärung muss u. a. in verständlicher Form und in einer klaren und einfachen Sprache erfolgen. Diese Merkmale sind insbesondere problematisch, wenn eine Einwilligungserklärung zugunsten mehrerer Unternehmen, hier acht Werbetreibende, eingeholt werden soll. Die Auflistung mehrerer Werbetreibender und ihrer jeweiligen Verarbeitungszwecke kann bereits zu einer komplexeren Einwilligungserklärung führen, die dann möglicherweise unverständlich sein könnte.

Das OLG Frankfurt a. M. hat im vorliegenden Fall mit Hinblick auf acht Werbetreibende keine Bedenken bezüglich der erforderlichen Klarheit gehabt. In diesem Zusammenhang hat das OLG Frankfurt a. M. festgestellt, dass die Unklarheit bezüglich eines Werbetreibenden nicht die Wirksamkeit der Einwilligung gegenüber einem anderen, genannten Werbetreibenden berührt.

Die Formulierung „Marketing und Werbung“ lasse bezüglich eines Werbetreibenden nicht erkennen, für welche Art von Produkten die Einwilligung in die Werbung erteilt wurde. Dies berühre nicht die Wirksamkeit der sachlich hinreichend konkretisierten Einwilligung(en) zugunsten der anderen Werbetreibenden (hier „Strom & Gas“). Die fehlende Erkennbarkeit der Verarbeitungszwecke eines Werbetreibenden führe nicht zu einer „Infizierung“ der gesamten Einwilligungserklärung auch hinsichtlich der übrigen Werbetreibenden.

Beweislast

Von Interesse sind auch die Ausführungen zur Beweislast. Das OLG Frankfurt a. M. sieht das sogenannte Double-Opt-in-Verfahren bei der Einwilligung in Telefonwerbung als „wenig beweiskräftig“ an.

Ein Gewinnspielteilnehmer konnte durch Markieren eines dafür vorgesehenen Feldes in dem betreffenden Teilnahmeformular angeben, dass er mit einem Werbeanruf einverstanden sei. Lag eine solche Einverständniserklärung vor, wurde dieser Teilnehmer durch einen gesonderten Anruf um Bestätigung seiner Einwilligung gebeten.

Im Gegensatz zum Double-Opt-in-Verfahren für den Erhalt von Werbe-E-Mails gebe es „zahlreiche, nicht fernliegende Gründe“ eine falsche Telefonnummer anzugeben. Nach dem OLG Frankfurt a. M. trage daher der Werbende die Darlegungs- und Beweislast dafür, dass der Telefonanschluss dem jeweiligen Gewinnspielteilnehmer zuzuordnen sei. Wenn der Werbende allerdings seiner Darlegungslast genügt hat, obliegt es wieder dem Angerufenen darzulegen, dass er dennoch keine entsprechende Werbeeinwilligung abgegeben hat.

Wettbewerbsrecht und DSGVO-Verstöße

Nach aktuellem Stand gibt es noch keine einheitliche Rechtsprechung, ob ein DSGVO-Verstoß über das Wettbewerbsrecht sanktioniert werden kann. Das OLG Frankfurt a. M. hat sich mit dieser Frage nicht beschäftigt. Die streitentscheidenden Normen sind im vorliegenden Fall zwar solche des UWG (insbesondere § 7 Abs. 2 UWG), diese finden ihre gemeinschaftsrechtliche Grundlage aber in der bislang nicht durch eine Verordnung abgelöste ePrivacy-Richtlinie (vgl. Art. 13 Richtlinie 2002/58/EG).

Praxistipp:
Das Urteil gibt Rechtsanwendern einen gewissen Gestaltungsspielraum (zurück). Es bleibt abzuwarten, ob andere Gerichte dieser Entscheidung folgen. Möglicherweise könnte, bei einer vertieften Auseinandersetzung mit dem sogenannten allgemeinen Kopplungsverbot eine abweichende Entscheidung ergehen. Bei unterschiedlicher OLG-Rechtsprechung wäre es am BGH und dem EuGH hier für eine abschließende Klärung zu sorgen.
Unternehmen sollten im Einzelfall prüfen, ob sie die Teilnahme an Gewinnspielen von einer Einwilligung, auch zugunsten mehrerer Werbetreibender, abhängig machen oder ob sie eine anderweitige Gestaltungsmöglichkeit wählen.

Dr. Stefan Peintinger, München
s.peintinger@skwschwarz.de

Zulässigkeit der GPS-Überwachung durch Unternehmen

In einem Urteil des Verwaltungsgerichts Lüneburgs vom 19.03.2019 (Az. 4 A 12/19) setzte sich das Gericht mit der datenschutzrechtlichen Zulässigkeit der GPS-Überwachung von Beschäftigten auseinander. Das Gericht verneint die gesetzliche Legitimation der damit einhergehenden Verarbeitung personenbezogener Daten und bezieht sich hierbei auf bereits bekannte Aspekte der Arbeitnehmerüberwachung. Die Entscheidung sollte jedoch nicht zu der Fehlvorstellung führen, dass jegliche GPS-Überwachung nun unzulässig sei. Gleichwohl gibt sie Anlass, dass Unternehmen die eigene diesbezügliche Praxis überprüfen.

Die Entscheidung:

Die Klägerin ist ein Unternehmen für Gebäudereinigung und hatte sämtliche betriebseigene Fahrzeuge mit GPS-Sensorik ausgestattet. Diese GPS-Sensorik erhob die Koordinaten jeder zurücklegten Strecke und speicherte diese für 150 Tage. Die Fahrzeuge wurden von Hausmeistern und Reinigungskräften genutzt und waren den jeweiligen betrieblichen Nutzern zugeordnet. Aufgrund eines Hinweises einer ehemaligen Mitarbeiterin leitete die zuständige Datenschutzaufsicht ein Verwaltungsverfahren ein und erließ nach Anhörung einen Bescheid gegen die Klägerin. Hierin stellte die Aufsichtsbehörde fest, dass die Erhebung und Speicherung von Positionsdaten in diesem Umfang nicht erforderlich sei und ordnete an, die Ortungssysteme so zu gestalten, dass eine personenbezogene Ortung während der ordnungsgemäßen betrieblichen Nutzung der Fahrzeuge nicht erfolgt.

Im anschließenden Gerichtsverfahren setzte sich das Gericht mit den Rechtsgrundlagen der Datenverarbeitung durch GPS-Systeme auseinander und kam zu dem Ergebnis, dass eine Erhebung und Speicherung der Positionsdaten nicht datenschutzkonform erfolge. Insbesondere eine Rechtfertigung nach § 26 Abs. 1 S. 1 BDSG verneinte es. Zwar besitze der Arbeitgeber auch schutzwürdige Interessen in diesem Zusammenhang, wie etwa die in der Verfassung verbriefte unternehmerische Organisationsfreiheit, eine Kontrolle des vereinbarten Umfanges der Nutzung sowie den Diebstahlschutz. Allerdings würden die vorgebrachten Argumente nicht greifen, da die Datenverarbeitung in diesem Umfang nicht erforderlich sei, um die jeweiligen Zwecke zu erreichen.

So sei für die Durchführung des Beschäftigungsverhältnisses von Hausmeistern und Reinigungskräften gerade keine lückenlose Kenntnis der Positionsdaten erforderlich, da die Daten „planungsunerheblich“ seien. Eine Kontrolle des zulässigen Umfanges der Nutzung sei nicht erforderlich, da die Beschäftigten die Fahrzeuge im begrenzten Maße auch privat nutzen dürften.

Ferner seien Ortungssysteme für einen präventiven Diebstahlschutz „völlig ungeeignet“. Es reiche vielmehr die im Falle eines tatsächlichen Diebstahles anlassbezogene Ortung aus.

Folgen für die Praxis:
Auch wenn die Entscheidung nicht vorbehaltlos auf jede standortbezogene Mitarbeiterüberwachung übertragbar ist, lassen sich aus der Entscheidung des VG Lüneburgs einige grundsätzliche diesbezügliche praxisrelevante Aspekte filtern. Die Entscheidung ist – unabhängig von der konkret eingesetzten Technik – dem Grunde nach auf sämtliche Unternehmen übertragbar, die Positionsdaten ihrer Beschäftigten verarbeiten, sollte jedoch nicht zu der Fehlvorstellung führen, dass eine GPS-Überwachung von Beschäftigten nun immer unzulässig sei. Vielmehr kommt es immer auf den jeweiligen Verarbeitungskontext wie die Branche sowie die konkrete technische Ausgestaltung an. Explizit angemerkt hat das Gericht etwa die Speicherfrist von 150 Tagen sowie dem Umstand, dass bei der erlaubten Nutzung des Fahrzeuges für private Fahrten, es in technischer Hinsicht erforderlich sei, dass zumindest im Rahmen einer solchen privaten Nutzung keine Standortdaten erhoben werden.

Eine gesetzliche Legitimation nach § 26 Abs. 1 S. 1 BDSG oder Art. 6 Abs. 1 lit. f DSGVO scheidet per se gerade nicht aus, auch wenn nicht unerhebliche Anforderungen angelegt werden. Nicht nachvollziehbar ist, warum das Gericht Positionsdaten vorbehaltlos als „planungsunerheblich“ bezeichnet hat, zumal die Verarbeitung von Beschäftigtendaten zu internen Verwaltungszwecken durch die Datenschutzgrundverordnung als berechtigtes Interesse explizit anerkannt ist. Der pauschale gerichtliche Hinweis auf die Führung von Fahrtenbüchern, die den unternehmerischen Interessen gleich gerecht würden, verkennt jedenfalls diese unternehmerische Organisationshoheit vor dem Hintergrund effizienterer technologischer Möglichkeiten. Hier wird es auf eine nachvollziehbare Argumentation gegenüber der Aufsichtsbehörde oder dem jeweiligen Gericht

ankommen. Als nicht praxistauglich gelten Einwilligungen, da diese jederzeit frei widerrufbar sind und daher keine verlässliche Basis für eine effiziente betriebliche Organisation darstellen.

Bedauerlicherweise keinen Anlass gab die Entscheidung für die Beurteilung von Betriebsvereinbarungen, die nach § 26 Abs. 1 S. 1 BDSG ebenfalls eigenständige Rechtsgrundlagen für die Verarbeitung von Beschäftigtendaten darstellen können. Unternehmen besitzen auch unter Geltung der Datenschutzgrundverordnung die Möglichkeit, für die Verarbeitung entsprechender Positionsdaten eine Betriebsvereinbarung abzuschließen. Soweit diese die höchstrichterlichen Vorgaben zur Arbeitnehmerüberwachung einhält, stellt sie eine taugliche Rechtsgrundlage zur Datenverarbeitung dar. Unternehmen, die die beschäftigtenbezogenen Vorgaben zur Arbeitnehmerüberwachung noch nicht umgesetzt haben, sollten die Hinweise des Gerichts zum Anlass nehmen, um den eigenen Umsetzungsstand kritisch zu überprüfen.

Dr. Hendrik Skistims, Frankfurt/Main
h.skistims@skwschwarz.de

EuGH zur datenschutzrechtlichen (Mit-)Verantwortung für Plugins und Drittinhalte

Der europäische Gerichtshof (EuGH) hat am 29.7.2019 eine wegweisende Entscheidung für Betreiber von Webseiten und Apps getroffen. Dabei geht es zum einen um die Einbindung von Plugins und Drittinhalten, zum anderen um die Frage, ob Datenschutzverstöße in Deutschland nach dem Gesetz gegen unlauteren Wettbewerb (UWG) abgemahnt werden können.

Ausgangspunkt ist ein Verfahren der Verbraucherzentrale NRW gegen einen deutschen Online-Händler. Die Verbraucherzentrale hat beanstandet, dass der Händler auf der eigenen Webseite den Facebook-Like-Button eingebunden hat, ohne dass die Benutzer der Webseite in die Datenübermittlung zu Facebook einwilligen mussten oder jedenfalls darüber aufgeklärt wurden. Der EuGH musste vor diesem Hintergrund entscheiden, ob Datenschutzverstöße überhaupt von Verbraucherschutzverbänden nach dem deutschen UWG abgemahnt werden können und ob der Onlinehändler für die Datenübermittlung und möglicherweise die Datenverarbeitung durch Facebook (mit-)verantwortlich ist.

Beim Facebook-Like-Button bindet der Betreiber der Webseite einen kurzen Code in seine Webseite ein, der eine Anwendung auf Servern von Facebook startet. Dabei kann Facebook auch dann Daten vom Besucher der Webseite erheben, wenn dieser gar nicht auf den Like-Button klickt, unter anderem die IP-Adresse, aber auch Daten über das genutzte Gerät. Sofern ein Nutzer selbst über ein Benutzerkonto bei Facebook verfügt, werden diese Informationen mit seinem Benutzerkonto geknüpft, aber auch wenn der Nutzer nicht bei Facebook registriert ist, werden seine Daten von Facebook verarbeitet. Im konkreten Fall hatte der Nutzer keine Möglichkeit, diese Datenübermittlung zu verhindern.

Das Verfahren war noch nach dem Recht der EU-Datenschutzrichtline von 1995 (RL 95/46/EG) zu entscheiden, nicht nach der EU-Datenschutz-Grundverordnung (DSGVO). Gleichwohl hat das Urteil auch unter der DSGVO erhebliche Bedeutung, da insbesondere die Regelungen zur gemeinsamen Verantwortung und die Rechtsgrundlagen im Wesentlichen unverändert aus der Datenschutzrichtlinie in die DSGVO übernommen worden sind.

Der EuGH hat entschieden, dass keine Mitverantwortung des Seitenbetreibers besteht, wenn er auf die tatsächliche Verarbeitung durch einen anderen Verantwortlichen keinen Einfluss hat, also die Zwecke und Mittel der Verarbeitung nicht bestimmt. Im konkreten Fall heißt das, dass der Online-Händler nicht für alle Datenverarbeitungen durch Facebook mitverantwortlich ist.

Allerdings meint der EuGH, dass der Händler durch die Einbindung des Plugins auf seiner Seite die Datenverarbeitung beeinflusst und daher die Mittel der Verarbeitung mit Facebook gemeinsam bestimmt hat. Hinsichtlich der Zwecke der Verarbeitung meint der EuGH, dass die Einbindung des Plugins der besseren Sichtbarkeit der Angebote des Händlers auf Facebook dient und daher der Händler und Facebook auch gemeinsam jedenfalls einen Zweck (Werbung) definiert haben. Allerdings schränkt der EuGH ein, dass das OLG Düsseldorf die konkreten Umstände nochmals genau zu prüfen hat.

Wenn schon die bloße Ermöglichung der Datenerhebung durch einen anderen Verantwortlichen zu einer gemeinsamen Verantwortung führt, läge eine solche wohl bei jeder Einbindung von Drittinhalten wie z. B. Videos, Bilder, Wetterberichten, Börsenkursen, etc. vor. Die Einbindung der Drittinhalte ermöglicht die Datenerhebung durch den Anbieter der Inhalte und wird meist auch im Interesse des einbindenden Webseitenbetreibers liegen.

Die Entscheidung enthält leider keine konkreten Kriterien für die Abwägung. Die Tatsache, dass dem Besucher der Seite im konkreten Fall gar nicht bewusst war, dass Daten an Facebook übermittelt werden, wird zwar mehrfach erwähnt, findet aber bei der Feststellung der gemeinsamen Verantwortung keine Berücksichtigung. Damit ist unklar, ob eine technische Einbindung, bei der eine Datenübermittlung an den anderen Verantwortlichen erst erfolgt, wenn der Besucher aktiv auf das Plugin oder den Drittinhalt klickt, datenschutzrechtlich anders zu beurteilen wäre. Das aktuelle Urteil des EuGH kann sogar so verstanden werden, dass jeder Link auf eine andere Webseite schon eine gemeinsame Verantwortung auslöst. Die Konsequenzen wären unüberschaubar.

Sofern die Datenverarbeitung auf ein berechtigtes Interesse gestützt werden soll, muss ein solches berechtigtes Interesse bei jedem der gemeinsam Verantwortlichen vorliegen.

Hinsichtlich der Abmahnfähigkeit von Datenschutzverstößen durch Verbraucherverbände hat sich der EuGH klar positioniert und die nationalen deutschen Regelungen für zulässig erachtet. Ob sich diese Einschätzung auch auf die heutige Rechtslage unter der DSGVO übertragen lässt ist fraglich, da sich die konkreten Regelungen inhaltlich unterscheiden und die DSGVO anders als die Richtlinie grundsätzlich vorrangiges Recht ist. Auch hier wird das Urteil in der Praxis für mehr Fragen sorgen als es Antworten geliefert hat.

Praxistipp:
Die Entscheidung erhöht die Haftungsrisiken von Seitenbetreibern bei der Einbindung von Plugins und Drittinhalten ganz erheblich. Derzeit bieten nach unserem Kenntnisstand Anbieter von externen Inhalten keine entsprechenden Vereinbarungen zur gemeinsamen Verantwortung an. In einem ersten Schritt sollten Seitenbetreiber daher prüfen, ob und ggf. welche externen Inhalte in der eigenen Seite integriert sind. Sofern weiter externe Inhalte wie Social-Media-Plugins, Kartendienste, Videos, Bilder, Webschriftarten, etc. in der eigenen Seite eingebunden bleiben sollen, raten wir dazu, diese jedenfalls erst nach einer aktiven Handlung der Besucher nachzuladen, z. B. durch Einbettung von Vorschaubildern, die die aktiven Inhalte erst nach einem Klick laden oder durch Verwendung von Lösungen wie der ursprünglich vom Heise-Verlag entwickelten Open Source Lösung Embetty (früher Shariff). In jedem Fall sollte die Datenschutzerklärung geprüft und ggf. ergänzt werden. Je nach Art des externen Inhaltes kann auch eine andere datenschutzrechtliche Gestaltung möglich sein, z. B. eine Auftragsverarbeitung. Sprechen Sie Ihre Inhaltslieferanten auf die EuGH Entscheidung an. Wir unterstützen Sie bei Bedarf gern.

Nikolaus Bertermann, Berlin
n.bertermann@skwschwarz.de

Do not remember me: The right to be forgotten & GDPR

German courts had a few opportunities to decide on cease and desist claims against search engines with the aim to block certain search results in connection with the claimant's name, a situation often associated with the right to be forgotten – or RTBF – as established by the ECJ. Delicate decisions need to be taken.

Most recently, the Regional Court of Frankfurt used Article 17 (1) GDPR as the legal bases for this (decisions dated 28 Feb 2019, case ref 2-03 O 315/17). It held that where a data subject may in certain in cases request deletion this implies that cease and desist from processing in the future can be claimed as well. The court arrived at this interpretation by autonomously construing European law.

Earlier this year, the Higher Regional Court of Dresden in a similar matter also reviewed Article 17 GDPR in this context (decisions dated 7 Feb 2019, case ref 4 W 1149/18), but had the dismissed the claim based on Article 17 para (3), arguing that in the present case the balancing of interests between such of the data subject and of the general public especially with a view to the function of search engines and their importance for freedom of information, went in favour of the search engines.

The decisions illustrate the real problem: search engines face the difficult task of assessing the balance of interests in each individual case. The German courts do provide some support to the engines by requiring that the claimant shows an infringement of rights which is “obvious and clearly recognizable at first sight”. However, even if this prerequisite is met the actual weighing of interests may still be difficult and delicate and is always treading the fine line between over-blocking and undue exposure.

Florian Hensel, München
f.hensel@skwschwarz.de

Die britische Datenschutzaufsicht kündigt über 200 Millionen Euro Geldbuße für British Airways an

Am 08.07.2019 hat die britische Datenschutzaufsichtsbehörde ICO (Information Commissioner’s Office) die Absicht mitgeteilt, gegen British Airways eine Geldbuße von über 200 Millionen Euro wegen Verstößen gegen die Datenschutz-Grundverordnung (DSGVO) zu verhängen. Darüber hatte British Airways bereits zuvor die Londoner Börse informiert.

Das Bußgeldverfahren wurde nach einer Anzeige im September 2018 eingeleitet. Nutzer wurden von Website und App der British Airways auf eine betrügerische Website umgeleitet, die mutmaßlich seit Juni 2018 persönliche Daten von etwa 500.000 Kunden „einsammelte“. Dazu gehörten gemäß ICO auch Log-in Daten, Kreditkartendaten und Reisebuchungen sowie Name und Adressinformationen. British Airways kooperierte mit der ICO und hat nach deren Auffassung unzureichende Sicherheitsvorkehrungen verbessert.

Gleichwohl informierte das ICO, dass eine Anhörung von British Airways zur beabsichtigten Geldbuße von 183,39 Mio. GBP (über 200 Mio. EUR) erfolgt. Nach dem Prinzip des One-Stop-Shop der DSGVO sei das ICO für die Sanktion des Datenschutzverstoßes von British Airways alleine zuständig. Nach der Mitteilung an die Londoner Börse über die angekündigte Geldbuße, die etwa 1,5 % des weltweiten Jahresumsatzes von British Airways im Jahr vor dem Verstoß entspricht, sank der Aktienkurs.

Das ICO hat die Geldbuße noch nicht verhängt. British Airways hat zuvor Gelegenheit zur Stellungnahme. Deren Muttergesellschaft hat bereits Maßnahmen gegen die Geldbuße angekündigt.

Praxistipp:
Datenschutzaufsichten verschärfen die Sanktionen für Datenschutzverstöße. Die französische Aufsicht verhängte 50 Millionen Euro Bußgeld gegen Google. Nun kündigt die britische Aufsicht über 200 Millionen Euro Bußgeld gegen British Airways an, die keine Vorteile aus dem Verstoß hatte. Auch in Deutschland laufen viele Bußgeldverfahren.
Für alle, die es (noch) nicht glauben wollen: Auch aus finanziellen Gründen empfiehlt es sich, die Anforderungen der DSGVO vollständig und genau umzusetzen.

Martin Schweinoch, München
m.schweinoch@skwschwarz.de