LOSCHELDER

Newsletter Datenschutzrecht
Januar 2019

Inhalt

Ist der Facebook „Gefällt mir“-Button datenschutzkonform als Marketinginstrument nutzbar?

Derzeit beschäftigt den EuGH ein weiteres datenschutzrechtlich bedeutsames Verfahren zu Social Media-Angeboten im Marketing: Welche Pflichten und Risiken treffen ein Unternehmen, das den „Gefällt mir“-Button von Facebook als Social Media-PlugIn auf seiner Website einbindet? Seit Kurzem liegen nun die Schlussanträge des Generalanwalts in diesem Verfahren vor (in vielen Fällen folgt das Gericht diesen Schlussanträgen), die für das künftige Marketing Licht- und Schattenseiten zugleich aufzeigen: Die datenschutzkonforme Nutzung von Social Media-Tools und ähnlichen Drittangeboten wird begrenzt; sie wird mit den jetzt vorliegenden Ausführungen aber auch rechtssicherer, wenn bestimmte Anforderungen eingehalten werden.

Die seit dem 19.12.2018 vorliegenden Schlussanträge des Generalanwalts Bobek (Rs. C-40/17) betreffen Fashion ID: Das Unternehmen hat den „Gefällt mir“-Button von Facebook als aktives Social Media-PlugIn auf seiner Website integriert, so dass Nutzer ein Kleidungsstück unmittelbar „Liken“ und so ihren Kontakten auf Facebook zeigen können. Der Button war als aktives PlugIn eingebunden, d.h. Nutzerdaten von Website-Besuchern (IP-Adresse, Cookies) wurden unabhängig davon an Facebook übermittelt, ob der Nutzer auf den „Gefällt mir“-Button klickt oder nicht. Dass eine solche aktive Einbindung datenschutzrechtlich riskant ist, war bereits vor Veröffentlichung der Schlussanträge bekannt und wird nun bestätigt. Vorzugswürdig ist die deaktive Einbindung mit transparenter Information darüber (insb. in der Datenschutzerklärung), da hierbei nur im Fall eines „Anklickens“ Daten des Nutzers an das Dritt-Unternehmen weitergeleitet werden; der Nutzer hat diese Weiterleitung damit selbst in der Hand.

Praktisch wesentlich ist: Die aktive Einbindung von Drittangeboten, bei denen schon beim Website-Besuch Daten an diese Drittanbieter übermittelt werden, ist nunmehr noch kritischer – es drohen bei einem Verstoß z.B. höhere Bußgelder, insbesondere, wenn der EuGH die Schlussanträge bestätigt. Sollen Drittangebote aktiv eingebunden werden, dann ist dies nur mit Einwilligung und frühzeitiger transparenter Information datenschutzrechtlich möglich. Die Schlussanträge sollten zum Anlass genommen werden, die eigenen (Online-) Marketing-Maßnahmen nochmals daraufhin zu untersuchen, ob personenbezogene Daten von (potentiellen) Kunden an Drittunternehmen weitergeleitet werden und, wenn dies der Fall ist, ob hierfür eine Erlaubnis (oder ein Auftragsverarbeitungsvertrag) gegeben ist sowie eine hinreichend transparente und frühzeitige Information erfolgt.

Grundlegend ist darüber hinaus, dass der Generalanwalt für eine klare Begrenzung des Bereichs plädiert, in dem eine gemeinsame Verantwortlichkeit besteht: Nur in den Phasen der Datenverarbeitung, in denen gemeinsam über Zweck und Mittel entschieden wird, sollen verschiedene Player auch wirklich gemeinsam verantwortlich sein. Am Beispiel des „Gefällt mir“-Buttons umfasst dies die Erhebung und Übermittlung von Daten an Facebook, da der Website-Betreiber diese aktiv durch Einbindung des PlugIns ermöglicht und im damit angestrebten Marketing ein gemeinsamer Zweck liegt. Die (gemeinsame) Verantwortlichkeit des Website-Betreibers soll dann dort enden, wo keinerlei Einfluss mehr auf die Datenverarbeitung durch das Drittunterneh-

men besteht. Diese Abgrenzung ist für die Praxis von enormer Bedeutung, zumal mit der DSGVO die gemeinsame Verantwortlichkeit einen Vertragsschluss erfordert und zur umfassenden Mithaftung im Außenverhältnis führt. Wenn der EuGH die Schlussanträge entsprechend klar bestätigt, wäre – wünschenswert – eine Mithaftung z.B. für einen späteren rechtswidrigen Umgang von Facebook mit über ein aktives PlugIn erlangten Nutzerdaten ausgeschlossen (zur Frage der gemeinsamen Verantwortlichkeit, Vertragsgestalten, Grenzen und Folgen demnächst auch umfassend Schreiber, Gemeinsame Verantwortlichkeit gegenüber Betroffenen und Aufsichtsbehörden, ZD 2/2019; das Manuskript hierzu wurde indes bereits vor Veröffentlichung der Schlussanträge verfasst).

Google in der Pflicht: Wie umfangreich ist das „Recht auf Vergessenwerden“?

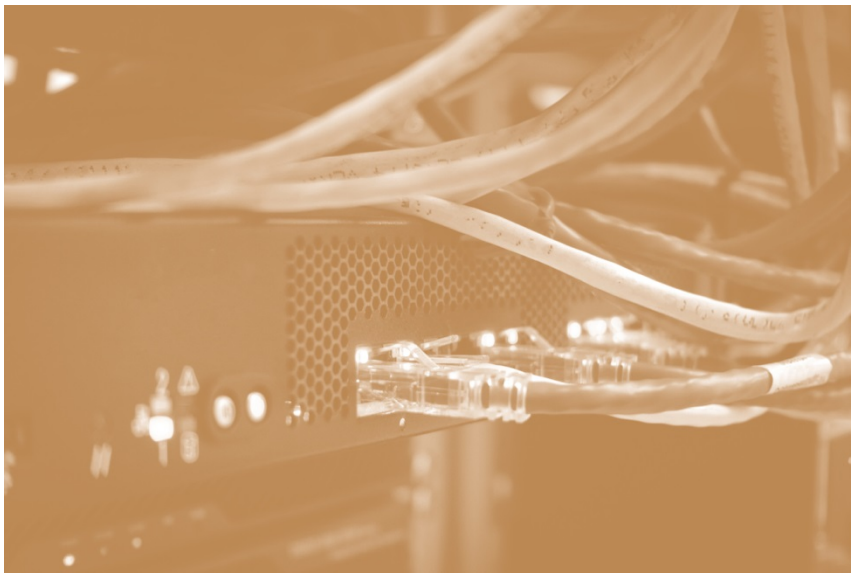
In zwei Schlussanträgen vom 10.01.2019 konkretisiert Generalanwalt Maciej Szpunar den Umfang des Rechts auf Vergessenwerden – in territorialer Hinsicht und mit Blick darauf, wie intensiv die Bemühungen des Verantwortlichen auf Löschung auch von Links ausfallen müssen, um sich datenschutzrechtskonform zu verhalten, jeweils bezogen auf den Suchmaschinenbetreiber Google.

Die seit dem 10.01.2018 vorliegenden Schlussanträge des Generalanwalts Maciej Szpunar (Rs. C-507/17 und Rs. C-136/17) betreffen Entscheidungen der französischen Aufsichtsbehörde (CNIL) – einmal ein gegen Google verhängtes Bußgeld und einmal die Weigerung, gegen Google einzuschreiten; sie sind bislang nur in französischer Sprache abrufbar.

Inhaltlich spricht sich der Generalanwalt zunächst für eine territoriale Begrenzung aus: Das Recht auf Vergessenwerden bestehe nur innerhalb der EU, also insbesondere nicht in Bezug auf in den USA gehostete Domains (.com). Eine weltweite Löschung käme allenfalls in Einzel-

fällen in Betracht. Allerdings soll der Verantwortliche verpflichtet sein, ihm mögliche Maßnahmen zu ergreifen, um innerhalb der EU für eine wirksame und vollständige Löschung zu sorgen, also u.U. auch über Geoblockingtechniken den Zugriff auf US-Suchergebnisse aus der EU heraus verhindern. In der zweiten Rechtssache konkretisiert der Generalanwalt das Recht auf Löschung, wenn besonders sensible Daten betroffen sind: Auch Suchmaschinenbetreiber müssten diese bei Vorliegen eines darauf gerichteten Antrags regelmäßig löschen, nur ausnahmsweise könne auf eine Abwägung zurückgegriffen werden, die im Ergebnis gegen eine Löschpflicht sprechen könnte.

Ob der EuGH sich den Schlussanträgen anschließt, bleibt abzuwarten; oft ist dies indes der Fall.



Umsetzungshilfe der LDI NRW für Datenschutzhinweise und Betroffeneninformation

Die Datenschutzgrundverordnung hat eine wesentliche Ausweitung der Informationspflichten mit sich gebracht: Bei jeder Datenerhebung und jeder Zweckänderung müssen Betroffene umfangreich nach Art. 13, 14 DSGVO über Umfang und Hintergründe der Datenverarbeitung unterrichtet werden. Für die praktische Abfassung dieser Datenschutzhinweise hat die NRW-Datenschutzaufsichtsbehörde jüngst eine Umsetzungshilfe veröffentlicht.

Die Umsetzungshilfe der LDI NRW ist abrufbar unter: https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/Informationspflichten-nach-der-Datenschutz-Grundverordnung/Umsetzungshilfe-Datenschutzinformationen_Stand-01_2019.pdf

Weiteres DSGVO-Bußgeld verhängt: 80.000 Euro wegen veröffentlichter Gesundheitsdaten

Wie erst kürzlich durch ein Zeitungsinterview mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg bekannt wurde, ist bereits ein weiteres Bußgeld wegen Verstoßes gegen die DSGVO verhängt worden: 80.000 Euro infolge einer Datenpanne, durch die Gesundheitsdaten versehentlich im Internet veröffentlicht wurden. Weitere Details, auch der Adressat des Bußgeldes, wird von der LfDI BW nicht genannt, da dies die Verletzung der Betroffenen weiter vertiefen könnte.

Informationen hierzu finden sich in dem Artikel der Esslinger Zeitung, abrufbar unter https://www.esslinger-zeitung.de/region/baden-wuerttemberg_artikel,-eu-datenschutzregeln-machen-viel-arbeit-aber-kaum%C2%A0abmahnungen-_arid,2237707.html

Neue und alte Probleme: Datenschutzrechtliche Risiken eines ungeregelten Brexit und vorläufige Absicherung des EU-US-*Privacy Shield*

Nach der Niederlage von Premierministerin May im britischen Unterhaus mehren sich die Befürchtungen, es könne Ende März 2019 zu einem „ungeregelten" Brexit ohne vertragliche Sonderregelungen kommen. Sollte es dazu kommen, bringt dies auch datenschutzrechtlich Handlungsbedarf mit sich, da das UK zu einem „Drittland" im Sinne der DSGVO würde. Der Datenaustausch mit den USA ist dagegen nach erneuter Prüfung durch die EU-Kommission vorerst weiterhin auf Basis des EU-US-Privacy Shield zulässig.

Die Übermittlung personenbezogener Daten in ein Drittland außerhalb der EU ist nur unter den zusätzlichen strengen Voraussetzungen der Art. 44 ff. DSGVO zulässig: Durch geeignete Garantieren muss ein angemessenes Datenschutzniveau im Zielland gewährleistet werden. Hinzu kommen Auswirkungen in anderen Bereichen, so müssten Datenschutzinformationen für die Betroffenen angepasst und u.U. aufgrund nun anderer Risiken eine Datenschutzfolgenabschätzung nach Art. 35 DSGVO durchgeführt werden.

Die Zusammenarbeit mit Unternehmen aus dem Vereinigten Königreich wäre vor diesem Hintergrund datenschutzrechtlich neu zu strukturieren: Um den konkreten Handlungsbedarf abzuschätzen, Handlungsoptionen zu identifizieren und diese rechtzeitig – u.U. vor dem 29.03.2019 – zu implementieren, sollte frühzeitig geprüft werden, ob personenbezogene Daten in das UK übermittelt und / oder dort verarbeitet werden, auch und vor allem durch Dienstleister wie Cloud- und Softwareanbieter.

Die vielfach von Unternehmen für einen Datentransfer in die USA herangezogene Zertifizierung nach dem EU-US-*Privacy Shield* hat derweil

eine Stärkung erfahren. Auch wenn das *Privacy Shield* derzeit vor dem EuGH angegriffen wird, kommt die EU-Kommission in ihrem Bericht über dessen zweite jährliche Überprüfung zu dem Ergebnis, dass ein angemessenes Schutzniveau für personenbezogene Daten weiterhin gewährleistet sei und dass das *Privacy Shield* daher im „Großen und Ganzen“ als Erfolg gewertet werden könne. Für Unternehmen eine gute Nachricht: Sie können bis auf weiteres auf Zertifizierungen ihrer Geschäftspartner nach dem *Privacy Shield* vertrauen und müssen nicht zwingend auf *Corporate-Binding-Rules* oder *Standardvertragsklauseln* zurückgreifen.

Transportverschlüsselung der Email-Kommunikation erforderlich

Nach der Landesbeauftragten für Datenschutz und Informationsfreiheit NRW müssen Unternehmen zum Schutz personenbezogener Daten ihre Email-Kommunikation mindestens mit einer Transportverschlüsselung sichern und sollten keine personenbezogenen Daten im Betreff aufnehmen; die Verschlüsselung soll entsprechend der Technischen Richtlinie „BSI TR-03108 Sicherer E-Mail-Transport“ implementiert sein. Daneben kann – je nach betroffenen Daten – eine Inhaltsverschlüsselung erforderlich werden.

Die Landesbeauftragten für Datenschutz und Informationsfreiheit NRW hat jüngst ihre Position zu den technischen Anforderungen an technische und organisatorische Maßnahmen beim E-Mail-Versand konkretisiert. Demnach ist regelmäßig eine Transportverschlüsselung erforderlich, die indes in den meisten Fällen ohnehin standardisiert angeboten wird.

Eine Inhaltsdatenverschlüsselung der Email-Kommunikation – beispielsweise über OpenPGP oder S/MIME – ist dagegen nur dann (zusätzlich) notwendig, wenn besonders schützenswerte Daten betroffen

sind (nach Auffassung der LDI NRW „z.B. Kontobewegungsdaten, Finanzierungsdaten, Daten zum Gesundheitszustand, Mandantendaten von Rechtsanwälten und Steuerberatern, Beschäftigtendaten“). Die Wirksamkeit einer Verschlüsselung via OpenPGP oder S/MIME war zwischenzeitlich in Frage gestellt worden; dies thematisiert die LDI NRW nicht. Allerdings weist die Aufsichtsbehörde darauf hin, dass unter Umständen – je nach Risiko für die Betroffenen – ein noch sicherer Übertragungsweg gewählt werden muss, etwa der elektronische Austausch über eine gesicherte Verbindung (Web-Portal des Verantwortlichen mit Zugangsbeschränkungen) oder die klassische postalische Zusendung.

Diese Position stellt noch nicht das letzte Wort in dieser Streitfrage dar. Die Datenschutzkonferenz arbeitet derzeit an ihrer Empfehlung zur datenschutzkonformen Email-Kommunikation. Es ist nicht ausgeschlossen, dass die Datenschutzkonferenz andere technische und organisatorische Maßnahmen zur Gewährleistung eines dem Risiko der Email-Kommunikation angemessenen Schutzniveaus nach Art. 32 Abs. 1 DSGVO empfiehlt.

Für alle weiteren Fragen rund um das Datenschutzrecht stehen Ihnen gerne zur Verfügung

Dr. Kristina Schreiber
+49(0)221 65065-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
+49(0)221 65065-200
simon.kohm@loschelder.de

Dr. Lucyne Ghazarian
+49 (0)221 65065-222
lucyne.ghazarian@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de