von **Dr. Bea Brünen**

Datenschutzgrundverordnung: Endet die Ära der Social Media Plugins?

Kaum eine Webseite kommt ohne Social Plugins von Facebook, Twitter & Co. aus. Webseitenbetreiber erhoffen sich durch den Einsatz der kleinen "Helferlein", dass User ihre Inhalte "liken" und "sharen" und sie so mehr Traffic auf ihren Seiten verbuchen können. Datenschützern sind Social Plugins jedoch schon seit langem ein Dorn im Auge. Der Grund: Sie sammeln - vom Webseitennutzer unbemerkt - personenbezogene Daten und können so detaillierte Persönlichkeitsprofile erstellen. Schiebt die Datenschutzgrundverordnung (DSGVO) der Nutzung von Social Plugins nun einen Datenschutz-Riegel vor?

A. Social Plugins: Zum Begriff und zur Funktionsweise

Facebook, Twitter, LinkedIn, Xing & Co: Fast jedes soziale Netzwerk bietet mittlerweile Webseitenbetreibern an, sogenannte Social Plugins auf ihren Webseiten einzubinden. Der Begriff "Social Plugins" meint dabei Erweiterungen für externe Seiten, die ein Teilen der Inhalte mit sozialen Gruppen ermöglichen sollen. Einer der wohl am weitesten verbreiteten Social Plugins ist zweifelsohne der Like-Button von Facebook. Da Social Plugins technisch grundsätzlich alle nach dem gleichen Prinzip funktionieren, wird im Folgenden die Funktionalität des Like-Buttons erläutert.

Damit Nutzer den Like-Button auf ihrer Webseite implementieren können, stellt Facebook ihnen einen Programmcode zur Verfügung, den diese in die HTML-Programmierung ihrer Webseite mittels eines sog. Iframes (=Inline-Frames) einbinden können. Die Einbettung eines Plugins hat zur Folge, dass bei jedem Aufruf der Internetseite automatisch und unabhängig davon, ob die Funktion "Gefällt mir" durch Anklicken genutzt wird, Daten an den Anbieter des Plugins übertragen werden. In jedem Fall werden mit Aufruf einer Seite bestimmte Grunddaten an Facebook übermittelt, jedenfalls die dynamische IP-Adresse des Nutzers und der String des genutzten Browsers.

B. Das Problem von Social Plugins nach bisheriger Rechtslage

Das Problem von Social Plugins wird aus der dargestellten Funktionsweise des Facebook-Like-Buttons schon relativ deutlich: Bei einer direkten Einbindung der Social Buttons auf der Shop-Seite stellen diese bereits beim "Betreten" der Webseite eine Verbindung zu den sozialen Netzwerken her. Facebook, Twitter & Co können so (vom Webseitenbesucher unbemerkt) Daten der Webseitenuser erheben und deren Nutzerverhalten tracken.

I. Datenschutz nur bei personenbezogene Daten

Der Anwendungsbereich des Datenschutzrechts ist nur eröffnet, wenn es sich bei den über Social Plugins erhobenen Daten um "personenbezogene Daten" handelt. Bei personenbezogenen Daten handelt es sich um Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 3 Abs. 1 Bundesdatenschutzgesetz (BDSG)). Wann genau Daten im Einzelfall als personenbezogen gelten, ist aufgrund dieser doch recht schwammigen Definition nicht immer eindeutig. Man kann sich jedoch merken, dass alle Informationen, über die irgendwie ein Personenbezug hergestellt werden kann, auch unter den Begriff der personenbezogenen Daten fallen.

Ob und in welchen Fällen Social Plugins personenbezogene Daten erheben, lässt sich am leichtesten am Like-Button von Facebook erläutern:

- Ist der Nutzer bei Facebook **eingeloggt**, können die über den Like-Button erhobenen Daten direkt mit ihm in Verbindung gebracht werden. **Klickt der User auf den Button**, kommt zusätzlich die Information hinzu, dass er einen bestimmten Inhalt gut findet. So lassen sich detaillierte Persönlichkeitsprofile erstellen, mittels derer insbesondere personalisierte Werbung an die Nutzer und deren Freundeskreis adressiert werden kann.
- Auch bei **nicht eingeloggten** Nutzern oder solchen **ohne Facebook-Account** findet bereits bei Seitenaufruf eine Datenübertragung an Facebook statt. Zu diesen übermittelten Daten zählt jedenfalls die **dynamische IP-Adresse** des Nutzers. Ob diese personenbezogen ist, war lange Zeit extrem umstritten. Der Knackpunkt dabei: Wer sich hinter der dynamischen IP-Adresse verbirgt, weiß in der Regel nur der jeweilige Internetzugangsanbieter des Nutzers und nicht der Webseitenbetreiber oder der Plugin-Anbieter. Dennoch hat der EuGH mit Urteil vom 19.10.2016 (C-582/14, Breyer/Bundesrepublik Deutschland) entschieden, dass dynamische IP-Adressen personenbezogene Daten sein können. Dies sei jedenfalls dann der Fall, wenn der Webseiten-Betreiber über rechtliche Mittel verfüge, mit denen er die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter (Access-Provider) dieser Person verfüge, bestimmen lassen könne. **Das bedeutet**: Verfügt der jeweilige Webseitenbetreiber über die rechtlichen Mittel (etwa

Auskunftsansprüche, vgl. Ziegenhorn, NVwZ 2017, 213, 217), um an die betreffenden Zusatzinformationen beim Access-Provider zu kommen, stellen dynamische IP-Adressen auch für den Webseiten-Betreiber personenbezogene Daten dar. Es ist momentan nicht abzuschätzen, wie Gerichte diese Auslegung des EuGH künftig in der Praxis handhaben werden und in welchen Fällen sie Webseiten-Betreibern die rechtlichen Mittel zusprechen.

Fest steht jedoch unterm Strich: IP-Adressen können personenbezogene Daten sein, sodass auch für Daten nicht eingeloggter oder nicht registrierter Webseitenuser das Datenschutzrecht greifen kann.

##II. Rechtfertigung der Erhebung von personenbezogenen Daten durch Social Media Plugins##

Die Erhebung und Verarbeitung personenbezogener Daten ist nach dem Telemediengesetz und dem BDSG grundsätzlich verboten. Zulässig ist sie nur dann, wenn sie durch Gesetz ausdrücklich erlaubt ist oder der Nutzer eingewilligt hat, § 12 Abs. 1 TMG, § 4 Abs. 1 BDSG. Es handelt sich jeweils also um ein Verbot mit Erlaubnisvorbehalt.

1. Daten für Betreib der Webseite notwendig

Zum Teil wird vertreten, dass die Erhebung und Verarbeitung personenbezogener Daten durch Social Media Plugins nach § 15 Abs. 1 TMG erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen oder abzurechnen (dazu Moser-Knierim, ZD 2013, 263; Ernst, NJOZ 2010, 1917, 1919).

Diese Auffassung wurde durch das LG Düsseldorf mit Urteil vom 09.03.2016 (12 O 151/15) abgeschmettert. Darin stellte das Gericht in Bezug auf den Facebook-Like-Button fest, dass der "Gefällt mir"-Button "für den Betrieb der Seite der Beklagten nicht unabdinglich" sei. Eine Webseite sei vielmehr "auch ohne Social Plugins zu betreiben und für die Nutzer aufzurufen."

Jedoch hat die Berufungsinstanz des LG Düsseldorf, das OLG Düsseldorf, dem EuGH eine Frage zur Auslegung des § 15 TMG vorgelegt. Mit dieser möchte das Gericht wissen, ob hinsichtlich der Erforderlichkeit der Datenverarbeitung durch Social Plugins auf die Interessen der Plugin-Anbieter (Facebook, Twitter & Co) oder auf die der Webseitenbetreiber abzustellen ist. Bis zur Klärung dieser Frage durch den EuGH bleibt die Rechtslage hier unklar.

2. Einwilligung in Datenübertragung

Unstreitig wird die Erhebung und Verarbeitung personenbezogener Daten über Social Plugins für zulässig erachtet, wenn der User eingewilligt hat.

Voraussetzung einer wirksamen Einwilligungserklärung ist aber nach dem BDSG, dass es sich um eine **aufgeklärte Willenserklärung** handelt. Sie muss freiwillig, für den konkreten Fall und in Kenntnis der Sachlage erfolgen (§?4a?BDSG). Dies erfordert jedoch, dass der Nutzer bereits im Rahmen der Einwilligung konkret und verständlich über die Datennutzungsvorgänge zu informieren ist, für die er seine Zustimmung erteilt. Diese sind möglichst genau zu bestimmen und müssen dem User eine informierte Entscheidung ermöglichen, seine Einwilligung im konkreten Fall zu erteilen oder zu versagen. Über die im Rahmen der Einwilligungserklärung aufgeführten Zwecke und Prozesse darf der Seitenbetreiber nicht hinausgehen, d.h. die Daten dürfen nur in dem Maße verwendet werden, wie sie von den in der Einwilligung ausgewiesenen Nutzungsvorgängen gedeckt sind.

Da im Bereich der Telemedien, insbesondere auf Websites, die Einholung einer schriftlichen Einwilligung gemäß § 4a Abs. 1 Satz 3 BDSG aus technischen und räumlichen Gründen von vornherein ausscheidet, lässt § 13 Abs. 2 TMG unter bestimmten Voraussetzungen auch eine **elektronisch eingeholte Einwilligung** in die Datennutzung zu. Danach wird eine elektronisch Einwilligung nur dann wirksam, wenn

- der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat **und**
- die Einwilligung protokolliert wird **und**
- der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann **und**
- der Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann.

Unterm Strich muss die Einwilligung freiwillig und informiert erfolgen. Die Einwilligung muss der Datenverarbeitung vorangehen und darf nicht erst nachträglich eingeholt werden. Die Einwilligung wiederum verlangt, dass der Nutzer über die Weitergabe seiner Daten vorher unterrichtet wird (vgl. LG Düsseldorf, Urteil vom 09.03.2016, 12 O 151/15).

In jedem Fall muss zudem die Datenschutzerklärung über die Datenerhebung, -verarbeitung und -nutzung aufklären.

C. DSGVO und Social Plugins

Am 25. Mai 2018 wird die Datenschutzgrundverordnung (DSGVO) in allen Mitgliedstaaten geltendes Recht. Anders als EU-Richtlinien, die durch die einzelnen Mitgliedstaaten erst noch in nationales Recht umgesetzt werden, sind EU-Verordnungen unmittelbar anwendbar. Das bedeutet: Die DSGVO gilt ab dem 25. Mai 2018 in Deutschland wie nationales Recht, Shop-Betreiber müssen die Regelungen ab diesem Zeitpunkt umsetzen.

Durch die DSGVO wird das Datenschutzrecht weitgehend reformiert. Einige Vorschriften des BDSG und des TMG werden durch die DSGVO ergänzt, andere werden weitgehend bestehen bleiben. Wiederum andere Regelungen des bisherigen Datenschutzrechts werden durch die DSGVO vollständig ersetzt. Welche Änderungen es konkret bezüglich der Nutzung von Social Plugins ab dem 25. Mai 2018 geben wird, erläutern wir im Folgenden.

I. Sachlicher Anwendungsbereich der DSGVO: Datenschutz nur bei personenbezogenen Daten

Ziel der DSGVO ist es, ein einheitliches Regelwerk in der ganzen EU zum Schutz personenbezogener Daten zu schaffen. Auch die datenschutzrechtlichen Vorgaben der DSGVO finden demnach nur Anwendung, wenn es sich bei den durch Social Plugins erhobenen Daten um personenbezogene handelt. Insofern ändert sich durch die DSGVO im Vergleich zur bisherigen Rechtslage in Deutschland nichts.

1. Personenbezogene Daten: Begriffsbestimmung

Personenbezogene Daten sind nach Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf eine **identifizierte** oder i*dentifizierbare* natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

2. Dynamische IP-Adressen als personenbezogene Daten?

Für die rechtliche Einordnung von Social Plugins ist insbesondere zu klären, ob die DSGVO dynamische IP-Adressen als personenbezogene Daten einordnet. Denn nur dann unterfallen auch Daten nicht eingeloggter oder nicht registrierter Webseitenuser dem Anwendungsbereich der DSGVO. Fraglich ist also, ob die hinter einer dynamischen IP-Adresse stehende natürliche Person "identifizierbar" ist.

Der Erwägungsgrund 26 zur DSGVO stellt darauf ab, dass die Identifizierbarkeit einer Person danach zu beurteilen ist, ob sie "der verantwortlichen Stelle [...] mit Mitteln möglich ist, die sie nach allgemeinem Ermessen wahrscheinlich nutzen" würde. Dies spricht dafür, dass es bei der Beurteilung der Identifizierbarkeit einer Person anhand einer IP-Adresse darauf ankommt, ob gerade die datenverarbeitende Stelle die Person identifizieren kann.

Andererseits stellt der Erwägungsgrund 26 alternativ auf eine nicht näher definierte "andere Person" ab, was dafür spricht, dass die theoretische (technische) Möglichkeit einer Identifizierung der Person unter Berücksichtigung des "gesamten Weltwissens" genügt.

In Bezug auf IP-Adressen normiert **Erwägungsgrund 30 zur DSGVO** jedoch konkret: "Natürlichen Personen werden unter Umständen Online-Kennungen wie IP-Adressen und Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, oder sonstige Kennungen wie Funkfrequenzkennzeichnungen zugeordnet. Dies kann Spuren hinterlassen, die insbesondere in Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der natürlichen Personen zu erstellen und sie zu identifizieren."

Daraus folgt: IP-Adressen sind nicht automatisch für jede Stelle personenbezogen. Dies spricht gegen einen absoluten Ansatz in der Form, dass bereits die theoretische Möglichkeit einer Identifizierung genügt.

Letztlich dürfte es darauf ankommen, ob der Webseitenbetreiber über die notwendigen Mittel verfügt, die ihm die Bestimmung der hinter den Daten stehenden Person grundsätzlich ermöglichen. Unerheblich dürfte also sein, ob die hinter den Daten stehende Person tatsächlich im konkreten Fall identifiziert wird. Entscheidend ist vielmehr, ob die Mittel den Webseitenbetreiber grundsätzlich hierzu in die Lage versetzen. Für diese Interpretation spricht auch die bereits oben genannte Entscheidung des EuGH vom 19.10.2016 (C-582/14, Breyer/Bundesrepublik Deutschland).

Fest steht jedoch auch hier unterm Strich: IP-Adressen können personenbezogene Daten sein, sodass auch für Daten nicht eingeloggter oder nicht registrierter Webseitenuser der Anwendungsbereich der DSGVO greifen kann.

II. Rechtfertigung der Erhebung von personenbezogenen Daten durch Social Media Plugins

Damit die Verarbeitung von personenbezogenen Daten rechtmäßig ist, muss mindestens eine der Voraussetzungen des Art. 6 Abs. 1 UAbs. 1 DSGVO vorliegen. Danach ist die Verarbeitung von Daten nur zulässig, wenn sie durch einen der gesetzlichen Tatbestände ausdrücklich erlaubt ist oder der Nutzer eingewilligt hat. Auch die DSGVO schreibt damit ein Verbot mit Erlaubnisvorbehalt fest.

1. Wahrung berechtigter Interessen

Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO ermöglicht die Datenverarbeitung ohne Einwilligung der Webseitenuser, wenn eine ausführliche Interessenabwägung zugunsten des Webseitenbetreiber ausfällt. Diese Vorschrift erlaubt die Verarbeitung personenbezogener Daten, wenn sie "zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich" sind, "sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen".

Es muss also zunächst ein berechtigtes Interesse vorliegen, zu dessen Wahrung die Verarbeitung erforderlich ist. Auch an dieser Stelle stellt sich zunächst die Frage, auf wessen berechtigtes Interesse konkret abzustellen ist: das Interesse des Plugin-Anbieters oder das des Webseitenbetreibers. Das OLG Düsseldorf hat dem EuGH eine Frage zur Auslegung des § 15 TMG vorgelegt, die auch für die Auslegung des "berechtigten Interesses" im Rahmen des Art. 6 Abs. 1 Uabs. 1 lit. f DSGVO relevant ist. Konkret möchte das Gericht wissen, ob hinsichtlich des berechtigten Interesses auf die Interessen der Plugin-Anbieter (Facebook, Twitter & Co.) oder auf die der Webseitenbetreiber abzustellen ist. Bis zur Klärung dieser Frage durch den EuGH bleibt die Rechtslage an dieser Stelle unklar.

Darüber hinaus ist nach dem Erwägungsgrund 38 "das Bestehen eines berechtigten Interesses besonders sorgfältig abzuwägen, wobei auch zu prüfen ist, ob eine betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird. Insbesondere dann, wenn personenbezogene Daten in Situationen verarbeitet werden, in denen eine betroffene Person vernünftigerweise nicht mit einer weiteren Verarbeitung rechnen muss, könnten die Interessen und Grundrechte der betroffenen Person das Interesse des Verantwortlichen überwiegen." Das bedeutet: Bei der Beurteilung, ob ein berechtigtes Interesse für die Erhebung von Daten durch Social Plugins vorliegt, ist auch einzubeziehen, ob der Webseitennutzer die Erhebung eben dieser Daten absehen kann bzw. mit dieser rechnen muss. In Bezug auf Social Plugins wird man wohl davon ausgehen müssen, dass die meisten User nicht damit rechnen, dass diese bei jedem Betreten einer Webseite Daten sammeln und auf diese Weise detaillierte Persönlichkeitsprofile erstellen können.

Ob Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO als Rechtsgrundlage zur Rechtfertigung der Datenerhebung herangezogen werden kann, ist somit stark zu bezweifeln.

2. Einwilligung in die Datenerhebung

Art. 6 Abs. 1 Uabs. 1 lit. a DSGVO ermöglicht eine Datenerhebung durch Social Plugins zudem, wenn die User eingewilligt haben. Danach ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat.

a. Informierte Einwilligung notwendig

Was die DSGVO konkret unter einer Einwilligung versteht, wird in Art. 4 Nr. 11 DSGVO definiert. Danach ist eine Einwilligung jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung. Eine bestimmte Form ist für die Einwilligung nicht vorgeschrieben. Erforderlich ist lediglich eine eindeutig bestätigende Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Auch die DSGVO verlangt somit (wie das BDSG und das TMG) eine **aufgeklärte Willenserklärung** des Users in die Datenerhebung und -verarbeitung. Die Einwilligung darf nicht pauschal, bspw. in Form einer Blanko-Einwilligung erfolgen. Sie muss vielmehr erkennen lassen, welche personenbezogenen Daten zu welchem Zweck von wem verarbeitet werden (vgl. Erwägungsgrund 32 zur DSGVO, dazu auch Ernst in: Paal/Pauly Datenschutzgrundverordnung 2017, Art. 4 DSGVO Rn. 78). Diese sind möglichst genau zu bestimmen und müssen dem User eine informierte Entscheidung ermöglichen, seine Einwilligung im konkreten Fall zu erteilen oder zu versagen.

b. Nachweispflicht

Art. 7 DSGVO normiert darüber hinaus weitere formelle und materielle Anforderungen an eine wirksame Einwilligung. Nach Art. 7 Abs. 1 DSGVO muss der Webseitenbetreiber **nachweisen**, dass der Webseitenuser in die Verarbeitung seiner personenbezogenen Daten eingewilligt hat.

c. Widerrufsrecht

Art. 7 Abs. 3 DSGVO normiert, dass die betroffene Person das Recht hat, ihre Einwilligung jederzeit zu widerrufen. Hiervon ist sie vor Abgabe in Kenntnis zu setzen. Der Webseitenuser muss also vor Beginn der Datenübertragung über die Social Plugins über sein Widerrufsrecht informiert werden. Art. 7 Abs. 3 DSGVO fordert zudem, dass der Widerruf der Einwilligung "so einfach" sein muss "wie die Erteilung der Einwilligung". Unzulässig wäre bspw., wenn ein Unternehmen für die Einwilligung einen bestimmten Ansprechpartner bestimmen würde und die Einwilligung nur diesem gegenüber widerrufen werden kann (vgl. Ernst in: Paal/Pauly Datenschutzgrundverordnung 2017, Art. 7 DSGVO Rn. 17).

III. Lösung der Problematik: Shariff und 2-Klick-Lösung

Bisher wurden zur rechtssicheren Einbindung von Social Plugins drei Varianten vorgeschlagen, deren Vereinbarkeit mit der DSGVO im Folgenden geprüft wird.

1. Verzicht auf Social Plugins

Die einfachste Lösung ist der Verzicht auf Social Plugins. Dies ist für die meisten Händler jedoch nicht sonderlich attraktiv, da sie sich der Marketing-Möglichkeiten der Verbreitung ihrer Angebote via sozialer Netzwerke nur sehr ungern entledigen möchten.

2. 2-Klick-Lösung

Eine weitere Lösung zur rechtssicheren Nutzung von Social Buttons bietet die sogenannte **2-Klick-Lösung** (LG Düsseldorf, Urteil vom 09.03.2016, 12 O 151/15). Bei der "2-Klick"-Lösung erscheint beim Seitenaufruf nicht unmittelbar das Social-Plugin des sozialen Netzwerks, sondern zunächst ein Hinweis, dass ein Symbol angeklickt werden müsse, um die Verknüpfung zum sozialen Netzwerk zu aktivieren. Klickt ein Nutzer sodann auf dieses Symbol, wird er zunächst gemäß den Anforderungen an eine informierte Einwilligung informiert. Erst wenn er durch einen 2. Klick bestätigt, dass personenbezogene Daten im Falle des Aktivierens des Social-Plugins übertragen werden, wird das betreffende Social-Plugin nachgeladen und eine Informationsübertragung an das soziale Netzwerk aufgebaut.

Die 2-Klick-Lösung dürfte grundsätzlich den Anforderungen an eine "eindeutig bestätigende Handlung" i. S. d. Art. 4 Nr. 11 DSGVO entsprechen. Dafür spricht insbesondere der Erwägungsgrund 32 zur DSGVO. Danach können User ihre Einwilligung etwa durch Anklicken eines Kästchens beim Besuch einer

Internetseite abgeben, mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert. Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person sollten nach Erwägungsgrund 32 zur DSGVO keine Einwilligung darstellen.

Problematisch dürfte jedoch sein, dass die Anbieter deutscher Websites "regelmäßig nicht in der Lage" sind, "die für eine informierte Zustimmung ihrer Nutzerinnen und Nutzer notwendige Transparenz zu schaffen" (vgl. Düsseldorfer Kreis am 08.12.2011). Denn: Eine **wirksame Einwilligung** setzt voraus, dass Nutzende wissen, **worin sie einwilligen**. Da Facebook aber bisher nicht offenlegt, welche Daten genau erhoben werden und was mit diesen geschieht, fehlt es an der nötigen Information, um eine informierte Einwilligungserklärung abgeben zu können.

Zudem muss die Einwilligung **nachweisbar** sein. Noch immer gilt grundsätzlich das Double Opt-In-Verfahren als einzige Möglichkeit, eine Einwilligungserklärung des Empfängers beweiskräftig zu beschaffen. Auch das bayerische Landesamt für Datenschutzaufsicht empfiehlt das Double-Opt-In-Verfahren für den Nachweis elektronisch eingeholter Einwilligungen (https://www.lda.bayern.de/media/ah_werbung.pdf, S. 11). Kaum jemand wird jedoch ein Double Opt-In-Verfahren bei Social Plugins installieren.

3. Shariff-Lösung

Die dritte Variante zur rechtssicheren Einbindung von Social Plugins stellt die sogenannte **"Shariff"-Lösung** dar. Bei dieser handelt es sich um eine Weiterentwicklung der "2-Klick"-Lösung, da sich im Produkteinsatz einige Nachteile für Webseitenbetreiber offenbart haben. Zum einen verleiten die Buttons nicht allzu sehr, Inhalte zu teilen, da zwei Klicks eine gewisse Hemmschwelle darstellen. Zum anderen springen die ausgegrauten Social Plugins nicht so sehr ins Auge wie die bunten Originale von Facebook, Twitter & Co.

Bei der Shariff-Lösung ruft ein Skript ab, wie oft eine Seite bereits geteilt oder getwittert wurde. Es nimmt über die Programmierschnittstellen (APIs) der Dienste zu diesen Kontakt auf und ruft die Zahlen ab. Die Abfrage geschieht also vom Server aus; statt der IP-Adresse des Besuchers wird lediglich die Server-Adresse an Facebook, Google und Twitter übertragen. Nutzer stehen erst dann mit Facebook, Google oder Twitter direkt in Verbindung, wenn sie aktiv werden. Vorher können die sozialen Netzwerke keine Daten über sie erfassen. **Das bedeutet**: Solange der Nutzer nicht auf den Link drückt, um Inhalte zu teilen, bleibt er für Facebook & Co. unsichtbar. Klickt der User auf den Link, liegt die Informationspflicht über die Datenerhebung und -verarbeitung aber nicht mehr beim Händler, sondern bei dem Betreiber des sozialen Netzwerkes.

D. Fazit

Die Ära von Social Plugins wird durch die DSGVO zwar nicht beendet. Da das Datenschutzrecht jedoch ab dem 25. Mai 2018 noch näher in den Fokus der Datenschützer gerückt wird, sollten Shop-Betreiber aktiv werden und entweder ganz auf Plugins verzichten oder auf die Shariff-Lösung zurückgreifen. Die 2-Klick-Lösung dürfte den Anforderungen der DSGVO nicht entsprechen und sollte daher nicht verwendet werden.

Autor:
Dr. Bea Brünen
(freie jur. Mitarbeiterin der IT-Recht Kanzlei)