von **Daniel Huber**

Facebook Connect: Das Single Sign On-Verfahren, Social Plugins und das Datenschutzrecht

Das Internet und der Datenschutz sind gegenwärtig nicht die allerbesten Freunde. Insbesondere soziale Netzwerke leben vom ständigen Austausch von Daten aus dem Netz, darunter vor allem personenbezogene Daten. Das deutsche Datenschutzrecht steht hingegen auf den Grundfesten der Datensparsamkeit und der möglichst informierten Entscheidung des Einzelnen darüber, was mit seinen personenbezogenen Daten geschieht. Sobald es zur Erhebung, Speicherung und Verwendung personenbezogener Daten kommt, muss der Betroffene darauf hingewiesen werden, und - wenn es keinen gesetzlichen Erlaubnistatbestand zur Datenverwendung gibt - um ausdrückliche Einwilligung gebeten werden. Viele Single Sign On-Verfahren halten sich nicht an dieses Credo und verstoßen daher gegen das deutsche Datenschutzrecht. Die IT-Recht Kanzlei erklärt, wo genau das datenschutzrechtliche Problem liegt und wie es sich unter Beibehaltung einer möglichst hohen Funktionalität am ehesten möglichst datenschutzrechtskonform lösen lässt.

I. Single Sign On und Social Plugins sind problematisch

Es ist praktisch für den Kunden und nützlich für Webshops sowie Social Media- und Internet-Plattformen: **Single Sign On-Verfahren** wie **Facebook Connect** oder Ähnliches von Twitter, Google+, Amazon sowie vielen anderen.

Das Prinzip ist einfach erklärt: Will ein Nutzer in einem Webshop bestellen, bei dem er noch kein Kundenkonto eingerichtet hat, so kann er den **Registrierungs- und Bestellprozess** dadurch **verkürzen**, dass er sich über ein in den Webshop integriertes Social Plugin mit seinem bereits bestehenden Facebook-, Amazon- oder sonstigen Account einloggt.

Anschließend werden personenbezogene Daten wie der Facebook-Name, die Nutzer-ID, das Alter, das Geschlecht, das Profilbild und die Freundesliste sowie die Gefällt-mir-Angaben von Facebook an den Webshop übertragen, der Kunde muss diese nicht mehr selbst händisch eingeben, sondern nur noch Fehlendes ergänzen. Kein lästiges Ausdenken eines neuen Nutzernamens und Passwortes mehr, **alles läuft nur noch über einen Login**.

Was derart praktische Vorteile hat, kehrt sich freilich in praktische Probleme um, sollte einmal der verknüpfende Social Media-Account abgeschaltet, gesperrt oder gehackt sein. Weitaus problematischer ist das Single Sign On-Verfahren jedoch für den beteiligten Webshop, da dieser **datenschutzrechtlichen Schwierigkeiten** ausgesetzt ist, die es zu lösen gilt.

II. Welche Daten werden bei Facebook Connect & Co transferiert?

Wenig überraschend ist Facebook mit seinem Single Sign On-Verfahren "Facebook Connect" der größte und am weitesten verbreitete Anbieter, weshalb er im Folgenden als Beispiel für die **datenschutzrechtliche Problematik** dienen soll.

Sobald sich ein Kunde via Facebook Connect auf der Webseite des entsprechenden Webshops eingeloggt hat, stellt der Webshop-Server mit den Facebook-Servern eine Verbindung her und tauscht Nutzerdaten aus. Die **öffentlichen** bzw. vom Nutzer als **öffentlich einsehbar deklarierten** Daten von Facebook wie der Facebook-Name, die Nutzer-ID, das Alter, das Geschlecht, das Profilbild und die Freundesliste sowie die Gefällt-mir-Angaben sendet Facebook an den Webshop.

Aber auch in die **umgekehrte Richtung** findet ein Datentransfer statt. Je nach Voreinstellung sendet der Webshop Informationen über das Surfverhalten des Nutzers im Webshop an Facebook, etwa für welche Produkte sich der Nutzer interessiert hat, welche Informationen er abgerufen hat und welche Waren oder Dienstleistungen er schließlich gekauft hat.

III. Der durch das Datenschutzrecht vorgegebene rechtliche Rahmen

Die Zulässigkeit der Erhebung, Speicherung, Nutzung und Verarbeitung von Daten im Internet richtet sich primär nach dem Telemediengesetz (kurz: TMG) und subsidiär nach dem Bundesdatenschutzgesetz (kurz: BDSG).

Nach § 12 TMG dürfen **personenbezogene Daten** zur Bereitstellung von Telemedien (u.a. Webseiten) nur erhoben und verwendet werden, soweit das TMG oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es **erlaubt** oder der Nutzer **eingewilligt** hat. Das TMG selbst erlaubt gemäß § 14 Absatz 1 TMG lediglich die Erhebung und Verwendung sog. personenbezogener Bestandsdaten, die für das Vertragsverhältnis mit dem Nutzer und damit für die Nutzung des Telemediums unbedingt erforderlich sind, und gemäß § 15 Absatz 1 TMG die Erhebung und Verwendung sog. personenbezogener Nutzungsdaten, insbesondere zu Abrechnungszwecken. In sonstigen Fällen der Erhebung und Verwendung personenbezogener Daten für die Nutzung von Telemedien ist somit die Einwilligung des betroffenen Nutzers erforderlich, der nach § 13 TMG möglichst umfassend über die Datenverwendung (insbesondere im Rahmen der obligatorischen Datenschutzerklärung) informiert werden muss.

Geht es nicht um (Vertrags-)Daten zur Bereitstellung von Telemedien (z.B. Vertragsschlüsse mit einem Musik- oder Video-Streaming-Dienst oder einem App-Portal), sondern beispielsweise zur Abwicklung eines Kaufvertrags mittels Lieferung physischer Waren, wie Schuhe und Kleidung, richtet sich die datenschutzrechtliche Zulässigkeit **nicht nach dem TMG**, sondern nach dem **BDSG**. Das Prinzip ist dort jedoch dasselbe: Für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten bedarf es nach § 4 Absatz 1 BDSG eines **gesetzlichen Erlaubnistatbestandes** oder einer **(informierten) Einwilligung** des Betroffen; dabei muss dieser vor seiner Einwilligung gemäß § 4a BDSG hinreichend über die Datennutzung (Datenschutzerklärung) informiert werden.

Zuständig für die Aufklärung wie auch für die sonstigen Pflichten nach dem BDSG ist die nach § 3 Absatz 7 BDSG verantwortliche Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

IV. Verstöße gegen das Datenschutzrecht durch Single Sign On-Verfahren

Bei Single Sign On-Verfahren wie etwa bei Facebook Connect finden diverse **problematische Datentransfers** statt.

- Mit **Einloggen** des Nutzers via Facebook Connect wird eine Verbindung zu den Facebook Servern aufgebaut und die IP-Adresse des Nutzers an Facebook übertragen. Folgt man der rechtlichen Ansicht, dass die IP-Adresse ein personenbezogenes Datum ist, ist bereits für diese Übertragung eine gesetzliche Befugnis oder die (informierte) Einwilligung des Nutzers erforderlich. Es kann hierbei wohl nicht davon ausgegangen werden, dass der Nutzer allein durch das Login bei Facebook eine informierte Einwilligung abgibt. Eine gesetzliche Befugnis hierzu fehlt; da der Nutzer nicht ausdrücklich darüber informiert ist, dass und an wen genau seine IP-Adresse übertragen wird, liegt auch keine hinreichende Einwilligung des Nutzers vor.
- Je nach **Konfiguration des Facebook-Accounts** und des Webshops sendet Facebook anschließend die **"öffentlichen" (personenbezogene) Daten** an den Webshop-Server. Welche konkreten Daten das sind, hängt davon ab, welche der Webshop-Server bei Facebook abfragt. Für diese Datenübertragung gibt es **keine** gesetzliche Befugnis, so dass als datenschutzrechtliche Rechtfertigung lediglich die **(informierte) Einwilligung** des Nutzers in Frage kommt. Zwar willigt der Nutzer durch das aktive Einloggen via Facebook Connect grundsätzlich in die Datentransfers zwischen Facebook und dem Webshop-Server ein. Jedoch weiß er zu diesem Zeitpunkt nicht, jedenfalls nicht genau, welche **konkreten personenbezogenen Daten** tatsächlich zwischen den Servern ausgetauscht werden, so dass er jedenfalls keine umfassend informierte Einwilligung trifft, solange ihn der Webshop nicht vor seinem Login möglichst genau darüber aufklärt. Ohne einen solchen Hinweis verstößt das Verfahren gegen deutsches Datenschutzrecht.
- Nach der Datenübertragung von Facebook auf den Webshop-Server werden die empfangenen Daten dort **gespeichert und ggf. weiterverarbeitet**. Für die Nutzung eines Großteils dieser Daten, die für das Vertragsverhältnis zwischen dem Nutzer und dem Webshop an sich nicht erforderlich sind (z.B. das Profilbild), gibt es keine gesetzliche Befugnis, so dass auch diesbezüglich der Nutzer eine informierte Einwilligung abgeben muss.
- Zum Abschluss **sendet der Webshop** je nach Konfiguration im Einzelfall eigene **Nutzungsdaten** wie das Surf- und Kaufverhalten des Nutzers zurück an die Facebook-Server. Wegen der Verknüpfung der Daten mit dem Facebook-Account des Nutzers haben diese einen konkreten Personenbezug, so dass es hierfür einer gesetzlichen Befugnis oder einer informierten Einwilligung bedarf, die gegenwärtig kaum jemand bedenkt.

Ein Webshop, der Facebook Connect (oder ein ähnliches Single Sign On-Verfahren) einsetzt, ist in Bezug auf die Datenabfrage von den Facebook-Servern, die Speicherung der empfangenen Daten auf den eigenen Webshop-Servern und die Sendung der Webshop-Nutzungsdaten des Nutzers zurück an Facebook die für den Datenschutz **verantwortliche Stelle** i.S.d. § 3 Absatz 7 BDSG und damit für die Einhaltung der einschlägigen Datenschutzbestimmungen **verantwortlich**.

Dies bedeutet, dass der Webshop für eine informierte Einwilligung des Nutzers im Vorfeld der Datentransfers sorgen muss, will er das Single-Sign On-Verfahren im Rahmen seines Webshops verwenden. Somit muss der Webshop-Betreiber eine **umfassende Datenschutzerklärung** verfassen und dafür sorgen, dass der Nutzer auf diese zwingend vor seinem Login via Facebook Connect (oder anderer entsprechender Verfahren) hingewiesen wird.

V. Keine datenschutzkonforme Verwendung von Facebook Connect & Co.?

Ob die Verwendung von Facebook Connect rechtskonform durchführbar ist, bleibt umstritten, eine belastbare Rechtsprechung zu diesem Thema existiert nach unserem Kenntsnisstand bislang noch nicht. Eine das rechtliche Risiko minimierende Lösung wäre die Implementierung des nachstehenden Verfahrens:

- Im Rahmen des Login-/Registrierungsprozess im Zusammenhang mit Facebook Connect müsste vom Nutzer zwingend eine **ausdrückliche Bestätigung** eingeholt werden, dass er zum einen darüber aufgeklärt wird, welche Datentransfers mit dem Verfahren wohin verbunden sind, und zum anderen, dass er mit diesen Datentransfers einverstanden ist.
- Zudem ist der Seitennutzer transparent im Rahmen der **Datenschutzerklärung** über die Datenverarbeitungsvorgänge im Zusammenhang mit Facebook Connect zu unterrichten.
- Die Einholung der Einwilligung sollte durch das Setzen eines Hakens in ein Kästchen erfolgen (sog. "Opt-In-Verfahren"), was der Webshop-Betreiber unbedingt **mitprotokollieren und speichern** müsste.
- Schließlich müsste die Einwilligung für den Nutzer leicht und formlos **widerrufbar** sein. Dies bedeutet, dass der Nutzer am besten in der Datenschutzerklärung auf die Möglichkeit des Widerrufs der Einwilligung hinzuweisen und ihm hierfür etwa eine E-Mail-Adresse zu nennen hätte.

Ob dieses Vorgehen einem gerichtlichen Verfahren Stand halten würde, lässt sich allerdings mit letzter Gewissheit nach dem gegenwärtigen Stand der Dinge nicht mit Sicherheit vorhersagen.

VI. Fazit

Das Single Sign On-Verfahren via Social Plugins wie Facebook Connect sind datenschutzrechtlich problematisch.

Zwar sind sie in aller Regel technisch so konzipiert, dass sie nicht bereits beim Aufrufen einer Webseite personenbezogene Daten an den jeweiligen Social Media-Server senden, sondern erst, wenn sich der Nutzer ausdrücklich für den Login mit seinem Account entschieden hat.

Allerdings wird der Nutzer im Laufe des Login-Prozesses in den meisten Fällen nicht oder zumindest nicht über das ganze Ausmaß der Erhebung, Speicherung und Nutzung seiner personenbezogenen Daten aufgeklärt. Da es zumindest für die Verwendung einer Großzahl der betroffenen Daten keinen gesetzlichen Erlaubnistatbestand gibt und insbesondere mangels ausreichender Aufklärung des Nutzers dieser keine informierte Einwilligung in die Verwendung seiner personenbezogenen Daten gibt, ist die Verwendung der Daten unzulässig, was sowohl zu Bußgeldern als auch zu Abmahnungen führen kann.

Die Entfernung solcher Single Sign On-Verfahren wäre nach gegenwärtigem Stand die einzige vollkommen rechtssichere Lösung, um eine Datenschutzrechtskonformität herzustellen. Wer durch geschickte Umgestaltung des Login-Prozesses dafür sorgt, dass der Nutzer eine informierte Einwilligung abgibt, und dies in seiner Datenschutzerklärung berücksichtigt, verstößt je nach konkreter Ausgestaltung im Einzelfall womöglich nicht gegen das Datenschutzrecht; allerdings bleibt ein Rest an Rechtsunsicherheit, solange die Rechtsprechung noch nicht entschieden hat..

Wichtig ist in jedem Fall die Beachtung des Grundsatzes, dass keine personenbezogenen Daten an Dritte (wie Facebook & Co) übermittelt werden dürfen, ohne dass der Nutzer im Vorfeld darüber in Kenntnis gesetzt worden ist und - im Zweifel - darin eingewilligt hat.

Bei Problemen, Rückfragen und weiteren Fragen zu diesem Thema hilft Ihnen das Team der IT-Recht Kanzlei selbstverständlich gerne auch persönlich und im Einzelfall weiter.

Autor:
Daniel Huber
(freier jur. Mitarbeiter der IT-Recht Kanzlei)