Social Media
Regeln beachten

[29.7.2016] Viele Behörden haben berechtigte Sorge, bei der Nutzung sozialer Medien gegen den Datenschutz zu verstoßen. Die Lösung ist jedoch nicht, sich Social Media komplett zu verweigern – sondern geeignete Bedingungen für eine regelkonforme Umsetzung zu schaffen.

Vor allem aufgrund datenschutzrechtlicher Bedenken schreitet die Nutzung von Web 2.0 und insbesondere der sozialen Medien in der öffentlichen Verwaltung kaum voran. Eine Verwaltung, die auf Bürgernähe und aufgabenorientierte Problemlösung ausgerichtet sein will, darf sich den sozialen Medien jedoch nicht völlig verweigern. Es gilt vielmehr, sich mit der Realität des Massenphänomens Social Media, den unterschiedlichen Umsetzungsvarianten sowie mit deren Implikationen und Rechtsfolgen auseinanderzusetzen. Auch aufgrund der Web-2.0-Evolution beschränkt sich die Rolle der Verwaltung im Internet nicht mehr auf bloße Präsenz und die Bereitstellung von Information – heute geht es um Kommunikation und Interaktion auf Augenhöhe. Über soziale Medien können Behörden ein breites, aber auch stark individualisierbares Publikum ansprechen. Konkret können Verwaltungseinheiten die sozialen Medien zu Werbezwecken nutzen, sie für größere Transparenz verwenden oder dort gezielt Dienstleistungen anbieten. Ebenso lassen sich E-Government-Ansätze verfolgen, dem Bürger können die Recherche von Informationen und der Zugang zu Dokumenten erleichtert werden. Zudem kann die Verwaltung soziale Netzwerke für den internen Austausch und eine tatsächliche Netzwerkbildung einsetzen. Wird die Nutzung sozialer Medien regelkonform ausgestaltet, schlägt die Verwaltung dadurch letztlich die goldene Brücke zum Bürger.

Problem des Social Log-in

Eine der beliebtesten Umsetzungsmöglichkeiten von Social Media ist der so genannte Social Log-in, eine Variante der Registrierung auf den unterschiedlichsten Web-Seiten mittels eines einzelnen Accounts in einem sozialen Netzwerk. Grundsätzlich fragt die administrierende Behörde bei der Registrierung für einen Dienst auf einer Website oder in einer App personenbezogene Daten ab. Seinen Abschluss findet dieser Vorgang meist durch einen Bestätigungslink, der an die E-Mail-Adresse des Registrierenden geschickt wird. Der Social Log-in ersetzt diesen Vorgang durch den Informationsaustausch über ein soziales Netzwerk. Dabei

werden die benötigten Daten an den Dienstanbieter übermittelt. Der Nutzer meldet sich also mittels seines Accounts im entsprechenden Netzwerk beim Dienst einer Behörde an. Technisch werden diese Log-in-Varianten als Social Plug-in in Form eines iFrames eingebunden. Das kann sich jedoch datenschutzrechtlich als problematisch erweisen. Zunächst werden die durch das soziale Netzwerk bereitgestellten Daten vom Dienstanbieter ausgelesen, etwa – Beispiel Facebook-Connect – Name, Vorname, Geburtstag, Geschlecht, Sprache, Profilbild, Titelbild, Social Media ID, Adresse, E-Mail-Adresse, Freundeslisten sowie "Gefällt mir"-Angaben. Der Dienstanbieter übermittelt dem Netzwerk seinerseits die von ihm gesammelten Daten. Ein solches Vorgehen widerspricht dem Grundsatz der Datensparsamkeit sowie dem Gebot der Zweckgebundenheit, denen die Verwaltung verpflichtet ist. Zudem kommt der Grundsatz des Verbots mit Erlaubnisvorbehalt zum Tragen: Demnach ist jede Verarbeitung personenbezogener Daten nur mit einer gesetzlichen Erlaubnis oder der Einwilligung des Betroffenen zulässig. Es erweist sich also als brisant, dass auch Registrierende betroffen sind, die eben keinen Gebrauch vom Social Log-in machen. So werden ohne Kenntnis des Nutzers bereits beim Aufruf der Verwaltungs-Website personenbezogene Daten erhoben, unter anderem die IP-Adresse – einfach durch eine Verbindung zur Seite des Social-Media-Anbieters.

Einwilligung unkompliziert einholen

Da in beiden Szenarien (mit und ohne Verbindung zum sozialen Netzwerk) sowohl die administrierende Behörde als auch der Anbieter des Netzwerks als verarbeitende Stelle im datenschutzrechtlichen Sinne auftreten, gelten für sie entsprechende Verpflichtungen. So bedürfen über Namen, E-Mail-Adressen und Geburtsdaten hinausgehende Daten einer Einwilligung durch den Betroffenen. Eine Datenschutzerklärung und die Einbettung einer interaktiven Einwilligungsoption für die Freischaltung des Social Log-ins sichern hier die Verwaltung als Dienstanbieter ab. Ähnliche Probleme wirft die Funktionalität des Sharing auf, eines der beliebtesten Marketingtools. Dabei wird der Besucher einer Website eingeladen, das angebotene Produkt oder die Dienstleistung mit dem eigenen Profil in einem sozialen Netzwerk zu verbinden oder zu bewerten – um letztlich ein User-Cross-Selling und Multiplikationseffekte zu erreichen. Auch hier werden Daten im bereits beschriebenen Umfang ausgetauscht. Allerdings lässt sich diesem Problem durch verschiedene technische Lösungen begegnen. Oft kommen so genannte Zwei-Klick-Lösungen oder skriptfreie Umsetzungen zum Einsatz. Ins

Blickfeld der Verwaltung gehört insbesondere die Zwei-Klick-Lösung, die eine Mitwirkungs- und Zwischeninstanz einbaut. Der Nutzer wird dabei aufgefordert, die Social-Media-Nutzung durch das Anklicken eines zusätzlichen Buttons freizuschalten. So werden nicht bereits beim Laden der Seite Informationen von anderen Servern abgerufen – oder zumindest deutlich weniger als ohne Zwei-Klick-Lösung. Das Resultat ist eine schneller geladene Seite mit weniger Overhead. Zugleich eröffnet das Mitwirkungselement dem Nutzer die Möglichkeit, sich der Datenerhebung zu entziehen. Eine Lösung rein auf Script-Seite vermeidet zwar den technischen Overhead, bringt aber keine datenschutzrechtlichen Vorzüge.

Mitarbeiter schulen

Ein erhebliches Gefährdungspotenzial ist zudem gegeben, wenn soziale Medien im Kontext verwaltungsrelevanter Beratungsleistungen genutzt werden. So wird die Reaktionszeit auf Posts vielfach als ein Qualitätsmerkmal gesehen. Dem Verwaltungsmitarbeiter bleibt bei seiner Reaktion daher kaum Zeit für eine Qualitätssicherung. Fehlt es jedoch an der entsprechenden Einweisung und Schulung, können die qualitativen Mängel einer Reaktion im Web desaströse Folgen im Kontext von Haftung und Marketing haben. Die Mitarbeiter zu involvieren, hat also ebenso zeitliche wie qualitative Implikationen. Datenschutzrechtlich wird dabei vor allem der Umgang mit erhobenen Daten relevant. Mitarbeiter des Verwaltungsapparats müssen sich bewusst sein, dass die Nutzung, Weitergabe oder gar Veröffentlichung personenbezogener oder personenbeziehbarer Daten stets an strikte rechtliche Rahmenbedingungen geknüpft sind. Anfragen oder Erhebungen dürfen – ohne entsprechende gesetzliche oder eine durch den Betroffenen vorgenommene Erlaubnis – nicht nach außen getragen werden. Eine persönliche Verwendung der Datensätze oder gar eine Vorteilsnahme dadurch ist unter allen Umständen zu unterbinden. Entsprechenden Risikoherden können Verwaltungsorganisationen entgegenwirken, indem sie Sensibilisierungsschulungen, Richtlinien und Best Practices als Standard einführen.

Risiken reduzieren

Festzuhalten bleibt, dass die Nutzung sozialer Medien Risiken birgt. Bei bewusstem und regelkonformem Vorgehen lassen sich diese jedoch gut und schnell handhaben oder ganz ausschließen. Die Führungsebene einer Organisation trägt die Verantwortung dafür, dass geeignete Rahmenbedingungen die Risiken

reduzieren. Ein wesentliches Element ist dabei ein nachhaltiges Informationssicherheitssystem mit einem umfassenden Datenschutz-Management, das ein Konzept zur Nutzung sozialer Medien beinhaltet. In ihm lassen sich Aspekte wie das Rechte-Management, Verantwortungen, Prozesse oder Kontrollinstanzen definieren. Zudem sind die Gestaltung und der Einsatz von Einwilligungsabläufen und Datenschutzerklärungen von höchster Relevanz.

Jan Alexander Linxweiler ist Associate bei Cassini Consulting.

Dieser Beitrag ist in der August-Ausgabe von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren. (Deep Link)

Stichwörter: Social Media

Bildquelle: PEAK Agentur für Kommunikation

Quelle: www.move-online.de