LEGAL WHITE PAPER

Rechtliche Aspekte von

Social-Media Management Tools

Christian Solmecke, LL.M.

Rechtsanwalt und Partner der Medienrechtskanzlei WILDE BEUGER SOLMECKE

WILDE BEUGER SOLMECKE
Rechtsanwälte
Kaiser-Wilhelm-Ring 27-29
50672 Köln
www.wbs-law.de

I. Überblick

In den letzten Jahren ist ein großer Markt um Software-Lösungen zum Management von Social-Media-Aktivitäten entstanden. Für Unternehmen sind die Tools attraktiv, da sie viele Prozesse vereinfachen und neue Möglichkeiten, z.B. beim Community Management und der Werbung bieten.

Generell ist der Einsatz eines Social-Media-Management-Tools regelmäßig mit der Erhebung und Verarbeitung einer Vielzahl von Daten verbunden. Dabei geht es insbesondere um die folgenden drei Bereiche:

- Speichern und Anzeigen von Daten der Mitarbeiter, z.B. Postings und Anzahl der Reaktionen/Beiträge/Likes auf diese (internes Tracking)
- Speichern und Anzeigen von Daten der Nutzer der jeweiligen Fan-Page, z.B. Namen und Postings (externes Tracking)
- Rechtliche Unterschiede zwischen der Nutzung eines Tools, das in Deutschland versus im Ausland (insbesondere in Irland) gehostet wird.

Der folgende Beitrag zeigt auf, wie ein gesetzeskonformes Social-Media-Management-Tool identifiziert werden kann bzw. worauf bei dessen Auswahl und Einsatz geachtet werden sollte. Dabei rückt insbesondere Facebook ins nähere Blickfeld, da die allermeisten Unternehmen hier den Großteil ihrer Social-Media-Aktivitäten verzeichnen bzw. Investments tätigen.

II. Internes Tracking

Grundsätzlich hat der Gesetzgeber die Erhebung und Verarbeitung von personenbezogenen Mitarbeiterdaten nur in engen Grenzen erlaubt. Regelmäßig ist eine solche nur dann erlaubt, wenn der Arbeitgeber ein besonderes Interesse an diesem Verfahren darlegen kann.

Einfachgesetzlich wurde die Erhebung und Verarbeitung von personenbezogenen Mitarbeiterdaten unter anderem an die Voraussetzungen des § 32 BDSG geknüpft. Danach ist die Erhebung und Verarbeitung von personenbezogenen Mitarbeiterdaten zulässig, wenn dies dem Zwecke des Beschäftigungsverhältnisses dient und für dessen Durchführung erforderlich ist. Personenbezogene Daten, die keinen Beschäftigungsbezug aufweisen und ausschließlich der Privatsphäre des Beschäftigten zuzurechnen sind, können vor diesem Hintergrund weder erhoben noch verarbeitet werden. Es ist jedoch anerkannt, dass der

Arbeitgeber ein berechtigtes Interesse an der Kontrolle der Beschäftigten hat, um festzustellen, ob sich die Beschäftigten entsprechend ihren vertraglichen Verpflichtungen und den Weisungen des Arbeitgebers verhalten. Im Gegenzug ist aber ebenfalls gebührend zu berücksichtigen, dass jeder Beschäftigte auch ein Recht auf informationelle Selbstbestimmung hat. Dieses verbietet eine dauerhafte, vollständige Überwachung eines Mitarbeiters (z. B. auch eine totale Videoüberwachung oder eine vollständige Überwachung der Telekommunikation). Das dadurch entstehende Spannungsfeld ist daher bei dem Einsatz technischer Einrichtungen wie einem Social-Media-Management-Tool zu beachten und interessengerecht aufzulösen.

Wichtig ist, dass das Social-Media-Management-Tool so konfigurierbar ist, dass mit ihm nur Daten erhoben und genutzt werden, die zur vollständigen Überwachung der Mitarbeiter nicht geeignet sind. Wir empfehlen im Standardfall ausschließlich folgende Daten zu erheben:

- Zeit des Ein- bzw. Ausloggens des Mitarbeiters
- Inhalt der Postings des Mitarbeiters
- Reaktion auf die Postings des Mitarbeiters (z.B. „Likes“)
- Anzahl der Aufrufe der Postings

Abhängig vom konkreten Beschäftigungsverhältnis können zudem auch folgende weitere Daten erhoben und verarbeitet werden:

- Zeit der Erstellung des Postings durch den Mitarbeiter

Darüber hinausgehende Daten dürften von dem Kontrollrecht des Arbeitgebers nicht mehr gedeckt sein. Insoweit wäre diese Erhebung und Verarbeitung der personenbezogenen Daten unzulässig. Ein Beispiel hierfür wäre:

- Eine vollständige Überwachung aller Arbeitsschritte, z.B. wann welche Kampagnen-Bilder im System hochgeladen oder editiert wurden

Weiterhin dürfen die erhobenen Daten aus Gründen der Datensparsamkeit nur über einen angemessenen Zeitraum gespeichert werden. Ein konkreter Zeitraum lässt sich daher nicht pauschal bestimmen. Vielmehr ist anhand der Arbeitsverträge zu ermitteln, welcher Zeitraum im Allgemeinen angemessen ist.

Zusätzlich ist darauf zu achten, dass die vom Arbeitgeber eingeführte Software vom Betriebsrat genehmigt wird, da diesem gemäß § 87 Nr. 6 BetrVG ein Mitbestimmungsrecht zusteht.

In der Praxis empfehlen wir die Beachtung folgender Aspekte bei der Auswahl eines Social-Media-Management-Tools:

- Konfiguration der Datenerhebung und -speicherung (siehe oben)
- Vorliegen einer wirksamen Auftragsdatenverarbeitung nach § 11 BDSG
- Anbieter ist durch Dritte geprüft, z.B. im Rahmen von ISO 27001
- Hosting der Daten in Deutschland (siehe Abschnitt IV)

Neben der hohen Rechtssicherheit werden so auch generelle Interessen von Mitarbeitern und ggf. Betriebsräten berücksichtigt – was wiederum elementar für eine unkomplizierte Einführung und nachhaltige Nutzung eines Tools ist.

III. Externes Tracking

Das Speichern von Nutzerdaten (hier: Namen und Postings), die z.B. auf einer Facebook-Fanpage oder mit einem Twitter-Tweet öffentlich geteilt werden, ist rechtlich unbedenklich soweit diese für die Markt- und Meinungsforschung verwendet werden. Für diesen Fall hat der Gesetzgeber in § 30a Abs. 1 Nr. 2 BDSG eine gesetzliche Erlaubnis normiert.

Ziel der Meinungsforschung ist allgemein die Ermittlung von Meinungen und Stimmungen der Bevölkerung. Meist geschieht dies durch entsprechende Befragungen von Mitgliedern der Bevölkerung, deren Daten sodann statistisch ausgewertet werden.

Der Betreiber einer Facebook-Fanpage ist legitimer Weise daran interessiert, die Stimmung der Nutzer hinsichtlich einzelner Postings oder der gesamten Fanpage zu erfassen. Nur so kann er adäquat mit seinen Fans interagieren. Einer Einwilligung des Nutzers bedarf es hinsichtlich der Erfassung und Verarbeitung dieser Daten bei öffentlich zugänglichen Facebook-Fanpages nicht. Ist die Fanpage hingegen nur für einen eingeschränkten, bestimmbaren Personenkreis erreichbar, so ist eine Speicherung der dort erlangten Informationen rechtswidrig.

Die erlangten Daten müssen gemäß § 30a Abs. 3 BDSG anonymisiert werden, sobald das Projekt der Markt- und Meinungsforschung eine solche Anonymisierung zulässt. Valide Datensätze für die Erforschung von Angebot und Nachfrage oder für die Bestimmung einer öffentlichen Meinung zu einem bestimmten Thema können erst nach einem bestimmten

Zeitraum gewonnen werden. Dieser Zeitraum unterliegt keinen starren Grenzen, sondern ist flexibel anhand der konkreten Fragestellung zu bestimmen. Es ist daher möglich, dass Daten auch über einen Zeitraum von einem Jahr gespeichert werden.

Nach § 30a Abs. 3 BDSG ist zu beachten, dass die personenbezogenen Daten zu anonymisieren sind, sobald dies nach dem Zweck des Forschungsvorhabens, für das die Daten erhoben worden sind, möglich ist. Auch an dieser Stelle muss daher wieder die konkrete Fragestellung der Markt- und Meinungsforschung betrachtet werden. So müssen zumindest diejenigen personenbezogenen Daten anonymisiert werden, die für die spezielle Fragestellung keinerlei Relevanz haben. So wird nach dem derzeitigen Wissensstand der Vor- und Nachname einer Person regelmäßig keine Bedeutung haben und deswegen zu anonymisieren sein.

Sobald der Nutzer einer Erhebung, Verarbeitung oder Nutzung seiner vorgenannten Daten jedoch gemäß § 20 Abs. 5 BDSG widersprochen hat, ist der Betreiber der Fanpage zur Löschung, jedenfalls aber zur Sperrung verpflichtet, sodass keine weitere Nutzung erfolgen kann.

Hinweis: § 30a BDSG sieht nicht die Nutzung der erhobenen Daten zu Werbezwecken vor. Sofern eine werbliche Nutzung der Daten erfolgt, müssen die strengen Regelungen des § 29 BDSG Beachtung finden. Hier ist generell zu empfehlen, dass gesonderte „Aktionen" durchgeführt werden, bei denen der Nutzer seine Daten selbstständig eingeben/übermitteln kann und dabei auch explizit das Recht zur werblichen Nutzung erteilt. Die Datenerfassung/-übermittlung kann z.B. über Formulare oder den „Facebook App Login" erfolgen. In der Praxis empfehlen wir auf folgende Aspekte bei der Auswahl eines Social-Media-Management-Tools besonders zu achten:

- Alle Punkte von II (siehe oben).
- \+ Möglichkeit, eigene Datenerhebungen/-abfragen durchführen zu können, z.B. über Landing Pages inklusive Teilnahmebedingungen, Opt-Ins etc.
- \+ Möglichkeit, erhobene Daten wieder löschen zu können.
- \+ Der Anbieter hat nur nach explizierter Freigabe Zugriff auf die durch den Auftraggeber erhobenen Daten (!).

Neben der hohen Rechtssicherheit werden so auch generelle Interessen von Mitarbeitern und ggf. Betriebsräten berücksichtigt – was wiederum elementar für eine unkomplizierte Einführung und nachhaltige Nutzung eines Tools ist.

IV. Datenschutzrechtliche Vorteile gegenüber einer Cloud im Ausland

Durch die steigende Anzahl von Anbietern von Social-Media-Management-Tools stellt sich vermehrt die Frage, welche Vorteile das Hosting einer Cloud-Lösung in Deutschland gegenüber einem Hosting im Ausland (hier am Beispiel Irland) hat.

Eine in Irland gehostete Cloud unterliegt grundsätzlich dem irischen Datenschutzrecht. Zwar gilt auch in Irland die Datenschutzrichtlinie (EU-Richtlinie 95/46/EG), jedoch entfaltet diese keine unmittelbare Bindung für den einzelnen Mitgliedstaat. Vielmehr hat jeder Staat bei der Umsetzung der Richtlinie einen gewissen Spielraum. Deutlich wird dies unter anderem bei der Sanktionierung von Datenschutzverstößen. Während dem Delinquenten in Irland nur vergleichsweise niedrige Bußgelder drohen, drohen ihm in Deutschland hingegen Bußgelder bis zu 300.000 € - eine empfindliche Strafe, die erfahrungsgemäß dazu führt, dass Anbieter mit einem Hosting in Deutschland sorgfältiger auf die Einhaltung des Datenschutzes achtet.

Weiterhin unterliegen Betreiber im Bereich des Anwendungsbereichs des deutschen Datenschutzgesetzes erheblich häufigeren und strikteren Kontrollen.

Allein aufgrund ihrer Kapazitäten kann die irische Datenschutzbehörde mit derzeit knapp 30 Mitarbeitern und ihrer Zuständigkeit für große Konzerne wie Facebook und Google nicht den Kontrollen in Deutschland die Stirn bieten. So verfügt in Deutschland allein die Dienststelle der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit über acht Fachreferate, den Bereich Zentrale Aufgaben und die Pressestelle. Der Mitarbeiterstab umfasst zurzeit etwa 90 Personen. Daneben verfügt auch jedes einzelne Bundesland über einen Datenschutzbeauftragten mit einem entsprechenden Mitarbeiterstab.

Randnotiz: Die Amazon Web Services (AWS) werden grundsätzlich auf mehreren Servern weltweit gehostet (US-Ost, US-West, EU, Asien-Pazifik, Südamerika). Bei der Einrichtung eines Services kann sich der Nutzer für eine Region (Availability Zone) entscheiden, in der seine Inhalte ausschließlich gehostet werden sollen. Diese Region ist nachträglich änderbar. Bei einer Entscheidung für ein Tool, das bei Amazon gehostet wird, sollte somit vertraglich geregelt sein wo genau die Software und Daten liegen und dass eine nachträgliche Änderung nur mit Zustimmung erfolgen kann.

Zusammenfassend lässt sich sagen, dass Anbieter und Nutzer, die Wert auf den bestmöglichen Schutz ihrer abgelegten Daten legen, auf Folgendes achten sollten:

- Standort der Cloud-Server ist bestenfalls in Deutschland.
- Es ist vertraglich zugesichert, dass der/die Server (Cloud) nicht verschoben werden.
- Ein formales Sicherheitskonzept für die Server, z.B. auch insbesondere bezüglich Zutritts-, Zugangs- und Zugriffskontrollen liegt schriftlich vor.

V. Fazit

Mit dem Einsatz von Social-Media-Managament-Tools sind rechtliche Risiken verbunden. Insbesondere die Möglichkeit mit dem Tool seine Arbeitnehmer vollumfänglich zu überwachen ist als sehr kritisch zu bewerten. Bei der Erfassung von Nutzerdaten ist daher darauf zu achten, welche Daten genau erfasst werden und ob sich diese jederzeit anonymisieren bzw. löschen lassen. Bezüglich des Hostings bieten in Deutschland betriebene Lösungen die größtmögliche datenschutzrechtliche Sicherheit.

Auf folgende Aspekte sollte bei der Auswahl eines Tools besonders geachtet werden:

- ❑ Eine Konfiguration der Datenerhebung und -speicherung ist möglich
- ❑ Es besteht die Möglichkeit, eigene Datenerhebungen/-abfragen durchzuführen, z.B. über Landing Pages inklusive Teilnahmebedingungen und der Möglichkeit Opt-Ins einzubauen
- ❑ Der Tool-Anbieter kann nur nach explizierter Freigabe durch den Auftraggeber auf die erhobenen und im System hinterlegten Daten zugreifen
- ❑ Es besteht die Möglichkeit, erhobene Daten auch wieder zu anonymisieren bzw. löschen
- ❑ Es liegt eine wirksame Auftragsdatenverarbeitung nach § 11 BDSG vor
- ❑ Das Hosting der Daten findet in Deutschland statt
- ❑ Es ist vertraglich zugesichert, dass der/die Server (bzw. Cloud) nicht verschoben werden
- ❑ Ein formales Sicherheitskonzept bzgl. Zutritts-, Zugangs- und Zugriffskontrollen liegt vor
- ❑ Der Tool-Anbieter ist durch unabhängige Dritte geprüft, z.B. im Rahmen von ISO 27001

Ein generelles (eher allgemeines) Qualitätsmerkmal ist zudem:

- ❑ Anbieter ist Teil eines offiziellen Partnerprogramms, z.B. Facebook PMD

Eine erste Analyse des Marktes zeigt, dass <u>nur ein einziger deutscher Anbieter</u> alle Anforderungen erfüllen konnte. Weitere deutsche Anbieter erfüllen die Kriterien zumindest teilweise. Demgegenüber weisen gerade ausländische Lösungen (hier: Dänemark, USA, Großbritannien, Frankreich, Benelux, und Finnland) eine Vielzahl an Mängeln im Sinne einer hohen Rechtsicherheit auf.