

MERKBLATT

Datenschutzkonforme Nutzung sozialer Medien durch öffentliche Organe

I. Einleitung

Dieses Merkblatt richtet sich an öffentliche Organe, welche der kantonalen Datenschutzgesetzgebung unterstehen und soziale Medien wie Twitter und Facebook nutzen.

Twitter und Facebook werden als Plattform für Veröffentlichungen und zum direkten Austausch mit Bürgerinnen und Bürgern genutzt. Mehrere Akteure (Plattformbetreiber, Provider, öffentliches Organ als Nutzender, Dritte als Nutzende) bearbeiten Informationen zu unterschiedlichen Zwecken. Auch unbeteiligte Dritte können von den Datenbearbeitungen betroffen sein. Im Folgenden werden die Rechtslage sowie Massnahmen für eine datenschutzkonforme Nutzung von Twitter und Facebook aufgezeigt. Grundsätzlich können diese Ausführungen auf andere soziale Medien wie LinkedIn, XING, Myspace und Youtube usw. übertragen werden. Es ist im Einzelfall abzuklären, ob Anpassungen notwendig sind.

Nicht thematisiert werden weitere Massnahmen, welche vor der Eröffnung solcher Accounts vorzunehmen, aber nicht unmittelbar datenschutzrelevant sind (Erarbeiten einer Strategie, Richtlinien für die Mitarbeitenden, Planung von Ressourcen usw.).

II. Rechtliches

Öffentliche Organe, welche auf Twitter und Facebook Dokumente veröffentlichen und interaktiv kommunizieren, müssen sich an den datenschutzrechtlichen Rahmenbedingungen orientieren. Kantonale Bestimmungen, welche vor der Eröffnung solcher „Accounts“ zu beachten sind wie beispielsweise Vorabkontrollen, sind vorbehalten.

1. Eröffnung eines „Accounts“

Der Nutzung dieser Plattformen liegt ein Vertragsverhältnis zwischen dem Betreiber der Plattform und dem öffentlichen Organ zugrunde, welches Elemente verschiedener Ver-

tragstypen aufweist. Das Vertragsverhältnis entsteht durch die Eröffnung eines „Accounts“ und dem damit verbundenen Akzeptieren der durch den Betreiber vorformulierten Allgemeinen Geschäftsbedingungen. Letztere werden spontan, einseitig und ohne Ankündigung periodisch geändert. Der Betreiber der Plattform speichert, analysiert und verwendet die Informationen auch zu eigenen Zwecken, ohne dass das öffentliche Organ Einfluss nehmen kann.

2. Veröffentlichungen

Eine Datenbekanntgabe setzt eine gesetzliche Grundlage oder die Einwilligung der Betroffenen voraus. Gesetzliche Grundlagen zur Veröffentlichung von Informationen finden sich in Datenschutz- und Informationsgesetzen sowie in fachspezifischen Erlassen. Willigt eine Person in eine Veröffentlichung ein, so muss diese Einwilligung in Kenntnis aller Konsequenzen, welche das Medium Internet beinhaltet, erfolgen.

Das Amtsgeheimnis und besondere Geheimhaltungspflichten wie beispielsweise das Steuergeheimnis können einer Veröffentlichung entgegenstehen.

Da Nutzende für den Zugang zu diesen Informationen auch eigene Daten bekanntgeben müssen, sind die Informationen der öffentlichen Organe auch auf andere Weise zugänglich zu machen.

3. Interaktive Kommunikation

Die Nutzung sozialer Medien soll nicht das Verwaltungshandeln ersetzen, sondern eine zusätzliche Plattform bieten, um schnell und umfassend über wichtige Belange zu informieren. Soziale Medien eignen sich nicht für hoheitliches Verwaltungshandeln. Der interaktive Austausch ist infolge der heiklen umfassenden Datenerfassung, –speicherung und Weiterbearbeitung durch die Betreiber auf ein Minimum zu beschränken. Wird die Grenze des niederschweligen Informationsaustausches überschritten oder handelt es sich um eine Rechtsanwendung im Einzelfall, so sind die Betroffenen auf die „üblichen“ Kanäle der Verwaltung zu verweisen (schriftliche Anfrage, Kontaktformular usw).

III. Verantwortung

Das öffentliche Organ ist für die auf die Plattform gestellten Inhalte verantwortlich. Eine Verantwortung besteht auch für die Nutzerkommentare. Daraus resultiert eine Bewirtschaftungspflicht.

Die Informationen müssen regelmässig auf persönlichkeitsverletzende und/oder strafrechtlich relevante Inhalte geprüft werden. Weiter sind Kommentare dahingehend zu sichten, ob sie für das Verwaltungshandeln relevant sind. Werden beispielsweise Informationszugangsgesuche über soziale Medien an das öffentliche Organ herangetragen, sind sie auf geeignete Weise zu beantworten (beispielsweise per Mail, falls Personendaten

betroffen sind oder in Papierform, falls die Antwort besonders schützenswerte Personendaten beinhaltet). Handlungsbedarf seitens des öffentlichen Organs kann unter Umständen auch entstehen, wenn Falschinformationen verbreitet und Dritte dadurch beeinflusst werden (beispielsweise wenn im Vorfeld von Abstimmungen irreführende Inhalte auf der Plattform veröffentlicht werden).

Das öffentliche Organ hat in einer Nutzungsregelung, welche auf der Plattform zu veröffentlichen ist, festzuhalten, wie es den „Account“ zu bewirtschaften gedenkt. Die Nutzenden können in diesem Rahmen auf Risiken in Bezug auf ihre Persönlichkeitsrechte hingewiesen und über Verhaltensempfehlungen informiert werden.

IV. Massnahmen

1. Vorabklärungen

Vor Eröffnung eines „Accounts“ hat sich das öffentliche Organ unter anderem Gedanken zu machen über:

- die Auswahl der sozialen Medien
- die Art der Nutzung
- das Ziel der Nutzung
- die Auswirkungen, welche die Eröffnung und insbesondere die Inanspruchnahme der interaktiven Kommunikation auf die Nutzenden hat
- Massnahmen, welche für eine datenschutzkonforme Nutzung umgesetzt werden müssen

Die Nutzung solcher Plattformen durch öffentliche Organe, welche fast ausschliesslich besonders schützenswerte Personendaten bearbeiten (beispielsweise eine psychiatrische Klinik oder eine Vollzugsanstalt) ist sorgfältig zu planen. Entsprechende Massnahmen, beispielsweise das Sperren der interaktiven Kommunikation, müssen Teil der Planung sein.

2. Nutzungsregelung

Das öffentliche Organ hat über die grundsätzlichen Aspekte der Nutzung Auskunft zu geben wie:

- Kontaktperson und Adresse
- Art, Umfang und Zweck der Nutzung
- Monitoringzeiten (im Normalfall im Rahmen der Bürozeiten)
- Art der Bewirtschaftung (Beantwortung der Kommentare nur im Rahmen des gesetzlichen Auftrags, Vorbehalt der Löschung von strafrechtlich relevanten und/oder persönlichkeitsverletzenden Inhalten, Protokollierung des Inhalts in diesen Fällen, Lösungsmechanismus usw.)

Über Gefahren wie beispielsweise die Speicherung, Auswertung und Weiterverwendung der Daten der Nutzenden durch den Betreiber ist ebenfalls zu informieren.

3. Monitoring

Ein „Account“ ist durch das öffentliche Organ aktiv zu bewirtschaften. Kommentare müssen gesichtet werden mit Blick auf:

- straf- und/oder zivilrechtlich relevante Einträge
- Anfragen, welche eine Verwaltungshandlung erforderlich machen
- Falschinformationen, welche sich auf die Veröffentlichungen des öffentlichen Organs beziehen und Dritte beeinflussen

Das Auswerten ist mit entsprechenden Programmen möglich. Kommentare mit politischem Inhalt oder anderen besonders schützenswerten Informationen dürfen nur ohne Bezug zur schreibenden Person ausgewertet werden. Ein umfassendes Monitoring des Nutzerverhaltens ist nicht erlaubt.

4. Löschen

Es ist zwischen dem Löschen durch den „Account“-Inhaber und dem Löschen durch den Betreiber zu unterscheiden.

Öffentliche Organe haben eine Pflicht zum Löschen von Informationen, wenn zivil- und/oder strafrechtlich relevante Äusserungen publiziert wurden. Weiter hat das öffentliche Organ Personendaten nach den kantonalen Vorgaben zu löschen.

Erfolgt ein Lösungsersuchen an den Betreiber, so besteht keine Gewissheit, ob die Informationen endgültig gelöscht wurden. Die Informationen sind in den meisten Fällen beim Betreiber weiterhin verfügbar.

5. Protokollieren

Werden widerrechtliche Inhalte durch das öffentliche Organ gelöscht, sind diese zur Nachvollziehbarkeit zu protokollieren. Die Aufbewahrung der Protokolle richtet sich nach den kantonalen Vorschriften.

6. Privacy Einstellungen durch öffentliche Organe

Im Folgenden die datenschutzrelevanten Einstellungen für Facebook:

Die Konfiguration erfolgt über die folgenden Schritte:

Administrationsbereich -> „Seite bearbeiten“ -> „Einstellungen bearbeiten“

Im Weiteren können folgende Optionen wahrgenommen werden:

- a) Unterbinden der Kommentare, Markieren und dem Schreiben von Nachrichten:
„Beitragsoptionen“, „Markierungserlaubnis“ und „Nachrichten“
- b) Kommentare vorgängig durch das öffentliche Organ freischalten:

„Standardsichtbarkeit der Beiträge anderer Nutzer in Chronik“ -> „Auf der Seite verbergen“

- c) Wortfilter aktivieren, um vulgäre Ausdrücke (u.a. in Kommentaren) zu blockieren:
„Blockierliste für vulgäre Ausdrücke“ -> „stark“

Twitter bietet keine Möglichkeiten, datenschutzrelevante Einstellungen vorzunehmen.

7. Einbindung von Social-Plugins

Die Einbindung von Social-Plugins ist datenschutzkonform, wenn diese unter hinreichender Information der Internet-Nutzenden und mit Einräumung eines Wahlrechts erfolgt. Eine intransparente und ungewollte Übermittlung der Nutzerdaten an die Betreiber ist zu verhindern, beispielsweise durch die „Zwei-Click-Lösung“. Siehe unter:

<http://www.edoeb.admin.ch/dokumentation/00153/00154/00167/index.html?lang=de>