Behörden-Leitfaden:

Umgang mit webbasierten sozialen Medien (Social Media)

5.09.2012

Niedersächsisches Ministerium für Inneres und Sport

Inhalt:

1. Zusammenfassung

Im Internet gibt es eine große Anzahl verschiedener Social-Media-Ausprägungen. Typische Ausprägungen sind soziale Netzwerke, Wikis, Blogs, Foren oder Newsgroups. Zur Zeit der Erstellung dieses Leitfadens sind z.B. das soziale Netzwerk Facebook, der Mikroblogging-Dienst Twitter und das Wiki Wikipedia besonders häufig frequentierte Social-Media-Angebote. Die Nutzung von Social Media bietet für die öffentliche Verwaltung interessante Chancen zur Verbesserung der Arbeitserledigung. Sie birgt aber auch zahlreiche Risiken. Dieser Leitfaden geht auf alle drei Dimensionen – Chancen, Risiken und Rechtsrahmen – ein, Schwerpunkt des Leitfadens ist jedoch, auf Gefahren und rechtliche Regelungen hinzuweisen und Maßnahmen zur Abwehr dieser Gefahren und zur Vermeidung von Rechtsverstößen zu beschreiben – um so das Risiko bei der Nutzung von Social Media in der öffentlichen Verwaltung zu minimieren.

Der Leitfaden richtet sich an die Behördenleitungen bzw. die Stellen, die über die Einrichtung bzw. Nutzung von Social Media entscheiden. Er soll aber auch den Beschäftigten des Landes Niedersachsen grundlegende Informationen für die Nutzung von Social Media geben. Der Leitfaden versucht so allgemein zu bleiben, dass die meisten Social-Media-Ausprägungen berücksichtigt werden.

Kapitel 3 des Leitfadens gibt einen Überblick über die Chancen, die Social Media bieten. Kapitel 4, 5 und 6 führen die Risiken auf und beschreiben wichtige rechtliche und organisatorische Regelungen. Kapitel 7 führt auf, welche Verhaltensregeln eingehalten werden sollen. Dabei beschreibt Kapitel 7.1 Regeln bei der Nutzung von Social Media und Kapitel 7.2 Regeln für Behördenauftritte in Social Media.

Im Anhang 1 des Leitfadens werden die unterschiedliche Web 2.0 – Ausprägungen kurz erläutert. Anhang 2 enthält die Bekanntmachung „Veröffentlichung von Beschäftigtendaten im Internet“ vom 23.01.2012. Anhang 3 listet in einem „Behörden-Leitfaden für Bedienstete“ die in Kapitel 7 aufgeführten Verhaltensregeln so auf, dass diese als Kurzfassung des Leitfadens weitergegeben werden können.

2. Einleitung

Nach der Verbreitung des World Wide Web Ende der 90er Jahre hat sich im Internet durch die Etablierung von Web 2.0 eine weitere tiefgreifende Fortentwicklung vollzogen. Web 2.0 ist ein vergleichsweise unbestimmter Sammelbegriff für neue webbasierte Dienste und Angebote sowie für ein neues Nutzerverhalten. Kern der Entwicklung ist eine grundlegende Erweiterung hin zu mehr Interaktion und Zusammenarbeit der Internetnutzerinnen und –nutzer, sowohl im privaten wie im beruflichen Bereich. Dabei beschränkt sich der Austausch nicht allein auf sachliche Informationen, vielmehr werden auch Profile, Emotionen, Meinungen, Eindrücke, Erfahrungen und Ideen übermittelt. Wesentlicher Gesichtspunkt und Unterschied zum Web 1.0 ist dabei eine stärkere Fokussierung am Dialog mit oder zwischen den Nutzerinnen und Nutzern. Diese Dienste und Angebote werden auch unter dem Begriff soziale Medien (Social Media) zusammengefasst.

Es gibt eine große Anzahl verschiedener Social–Media-Ausprägungen im Netz. Zu den einzelnen Ausprägungen gibt es verschiedene Angebote. Nicht immer ist die Bewertung einfach, ob eine Ausprägung überhaupt zu den Social Media gehört. Auch entwickeln sich die Ausprägungen und Angebote ständig fort und werden durch neue ergänzt. Typische Ausprägungen sind soziale Netzwerke, Wikis, Blogs, Foren oder Newsgroups. Zur Zeit der Erstellung dieses Leitfadens sind z.B. das soziale Netzwerk Facebook, der Mikroblogging-Dienst Twitter und das Wiki Wikipedia besonders häufig frequentierte Social-Media-Angebote. Ein Überblick über Social-Media-Ausprägungen und -Angebote sind in Anhang 1 aufgeführt.

Die Nutzung von Social Media bietet für die öffentliche Verwaltung interessante Chancen zur Verbesserung der Arbeitserledigung. Eine wachsende Anzahl von Behörden, sowohl in Kommunal- als auch in Landesverwaltungen nutzt diese zusätzlich zur vorhandenen Internetrepräsentanz. Sie birgt aber auch zahlreiche Risiken. Dieser Leitfaden geht auf alle drei Dimensionen – Chancen,Risiken und Rechtsrahmen – ein, Schwerpunkt des Leitfadens ist jedoch, auf Gefahren und rechtliche Regelungen hinzuweisen und Maßnahmen zur Abwehr dieser Gefahren und zur Vermeidung von Rechtsverstößen zu beschreiben – um so das Risiko bei der Nutzung von Social Media in der öffentlichen Verwaltung zu minimieren.

Der Leitfaden richtet sich an die Behördenleitungen bzw. die Stellen, die über die Einrichtung bzw. Nutzung von Social Media entscheiden. Er soll aber auch den Beschäftigten des Landes Niedersachsen grundlegende Informationen für die Nutzung von Social Media geben. Für diese ist in Anhang 3 auch eine Kurzfassung des Leitfadens beigefügt, die lediglich die Verhaltensregeln beim Umgang mit Social Media aufführt.

Der Leitfaden versucht so allgemein zu bleiben, dass die meisten Social-Media-Ausprägungen berücksichtigt werden. Betrachtet werden in erster Linie Angebote im Internet. Grundsätzlich werden aber auch Intranet-Angebote mit einbezogen.

Der Leitfaden wurde vom Niedersächsischen Ministerium für Inneres und Sport erstellt und am 4.09.2012 vom Niedersächsischen IT-Planungsrat zustimmend zur Kenntnis genommen. Er ist somit eine abgestimmte Empfehlung der Niedersächsischen Ressorts zum Umgang mit webbasierten sozialen Medien und ist in diesem Sinne von der Landesverwaltung zu berücksichtigen.

3. Chancen: Wie kann die öffentliche Verwaltung Social-Media-Angebote nutzen?

Neben dem Angebot von Informationen bietet die Internet-Technik verschiedene Möglichkeiten, dass beliebige Nutzerinnen und Nutzer Daten über das Internet bereitstellen. Die verschiedenen Social-Media-Ausprägungen nutzen diese Möglichkeiten auf vielfältige Weise. Die so entstandenen Angebote zeichnen sich meist dadurch aus, dass sie einfach nutzbar und kostenlos[1] sind. Sie sprechen oft besondere Zielgruppen an. U.a. durch diese Eigenschaften haben sich viele Angebote zu Trendmedien entwickelt. Besonders für viele Jugendliche und junge Erwachsene sind diese Medien zur entscheidenden Informationsquelle und zur zentralen Kommunikationsplattform geworden.

Die öffentliche Verwaltung kann die Social-Media-Angebote für ihre Aufgabenerfüllung auf vielfältige Weise nutzen. Sie muss sich teilweise sogar darauf einstellen, dass die Social-Media-Nutzung und -Präsenz von ihr erwartet wird. Repräsentanzen bis hin zu „Fanseiten" werden tatsächlich bereits von Hochschulen, Landesregierungen, der Polizei und anderen bereitgestellt.

Prinzipiell bieten sich für die öffentliche Verwaltung die nachfolgenden Einsatzgebiete besonders an, wobei stets die im Anschluss erläuterten Risiken zu beachten sind:

<u>„Passive" Informationsbeschaffung</u>

Social Media sind zunächst eine neue, wichtige Quelle für die Recherche nach Informationen für die Aufgabenerledigung der Verwaltung – also für das Wissensmanagement. Z.B. hat die als Wiki betriebene Online-Enzyklopädie Wikipedia eine wichtige Rolle bei der ersten Informationsbeschaffung eingenommen. Zahlreiche Foren liefern auch der Verwaltung wichtige Informationen. Die Medien zur Informationsbeschaffung können oft ohne eine Anmeldung bzw. Identifizierung oder eine eigene Präsenz im Internet genutzt werden. Im einfachsten Fall werden die relevanten Informationen als Treffer über eine Internet-Suchmaschine angezeigt.

Beteiligte in der Verwaltung: Bedienstete mit Internet-Zugang

<u>Presse- und Öffentlichkeitsarbeit</u>

In der Presse- und Öffentlichkeitsarbeit ist es wichtig, dass Informationen schnell, gut aufbereitet und authentisch den gewünschten Adressatenkreis erreichen und von diesem möglichst umfassend wahrgenommen werden. Social-Media-Angebote erlauben es meist, Informationen vergleichsweise einfach und kostengünstig im geeigneten Format[2] ins Netz zu stellen. Durch die Wahl des Mediums lässt sich steuern, welcher Adressatenkreis die Informationen in erster Linie wahrnimmt. Darüber hinaus ermöglichen die sozialen Medien häufig, dass Angebote kommentiert und weitergeleitet werden. Dies ermöglicht eine effektive Verbreitung von Informationen und eine Rückkopplung, welche Informationen besonderes Interesse finden. Durch Funktionen wie beispielsweise „Teilen", „Gefällt mir" und „Freunde" können die Bürgerinnen und Bürger eine Rückmeldung geben oder für eine gezielte Weiterverbreitung an die eigenen sozialen Verknüpfungen sorgen.

Beteiligte in der Verwaltung: Pressestelle, Behördenleitung, Fachbereiche

---

[1] Sie finanzieren sich meist durch Werbung.
[2] Hierzu gehören nicht nur Texte, sondern auch Bilder und Podcasts.

Bürgerkommunikation

Geeignete Social-Media-Angebote können für die direkte Kommunikation mit Bürgerinnen und Bürgern, etwa zur Beantwortung von Bürgeranfragen oder für das Beschwerdemanagement eingesetzt werden. Solche Angebote können dazu beitragen, „Bürgernähe“ zu zeigen und z.B. die Akzeptanz von neuen Vorhaben zu verbessern. Sie können den Aufwand für schriftliche Informations- oder Beteiligungsverfahren deutlich reduzieren. Für ein „Open Government“ ließen sich neue Plattformen erstellen, die gleichzeitig Werbeeffekte, Transparenz, Netzwerkbildung und auch sonst Möglichkeiten eines Dialogs ohne formelle Hürden begünstigen.

Beteiligte in der Verwaltung: u.a. Bürgerbüro, Service-Center

„Aktive“ Informationsbeschaffung

Social-Media-Angebote eignen sich im besonderen Maße für eine direkte Aufforderung zur Information, soweit dies rechtlich zulässig ist. Fragen lassen sich leicht erstellen und verteilen. Nutzerinnen und Nutzer können vergleichsweise einfach antworten.

Beteiligte in der Verwaltung: Bestimmte Fachbereiche

Fachlicher Diskurs

Social Media bieten fachlichen Experten in der Verwaltung die Möglichkeit, mit anderen Fachleuten oder Interessierten Wissen und Meinungen direkt auszutauschen. Dies ergänzt den traditionellen Informations- und Meinungsaustausch über Fachartikel, Vorträge oder Podiumsdiskussionen. Von Vorteil ist, dass die Fachleute örtlich unabhängig, jederzeit und mit wenig Aufwand an diesem fachlichen Diskurs teilnehmen können. Im Idealfall können auf diese Weise Ergebnisse erzielt werden, die ansonsten gar nicht oder nur mit hohem zeitlichen und finanziellen Aufwand erzielt werden könnten (im Sinne von crowd sourcing[3]).

Beteiligte in der Verwaltung: „Experten“ der Verwaltung

Kommunikation im Intranet

Die aufgeführten Möglichkeiten der Social-Media-Nutzung können auch in internen Arbeitsprozessen genutzt werden, insbesondere in größeren Verwaltungen. Auch in einem Intranet können z.B. Foren oder Wikis betrieben oder in neuen Formen „offene Kommunikation“ erprobt werden. Durch die Begrenzung der Zugriffsberechtigung auf die Verwaltung kann hier prinzipiell – unter Beachtung der datenschutzrechtlichen und der geheimschutzrelevanten Einschränkungen - offener kommuniziert werden, was für das Wissensmanagement von großem Vorteil sein kann. Voraussetzung hierfür sind natürlich ein entsprechendes Intranet-Angebot und die Bereitschaft der Bediensteten dieses zu nutzen.

Beteiligte in der Verwaltung: Praktisch alle Bediensteten

[3] Als crowd sourcing bezeichnet man die Auslagerung von Aufgaben auf die Intelligenz und die Arbeitskraft einer Masse von Freizeitarbeitern im Internet.

4. Risiken: Gefahren und deren Auswirkungen bei der Nutzung von Social Media

Mit der Nutzung von Social Media sind nicht nur Chancen, sondern auch Risiken verbunden. Dies gilt in besonderem Maß für die öffentliche Verwaltung. Wenn sich Bedienstete einer Behörde in Social-Media-Angeboten äußern, sei es als Nutzer oder Nutzerin mit Bezug zu einer Behörde oder als Autoren einer Behördeninformation, so muss davon ausgegangen werden, dass diese grundsätzlich als öffentliche Äußerungen der Behörde wahrgenommen werden. Unbedachte bzw. falsche Äußerungen können nicht nur ein negatives Presseecho zur Folge haben, sondern auch Personen schädigen, die gemäß diesen Äußerungen handeln. Unter Umständen sind hiermit Schadensersatzforderungen verbunden. Unbedachte Äußerungen können auch dazu führen, dass kriminelle Handlungen erleichtert bzw. angeregt werden.

Außerdem können öffentliche Äußerungen gegen gesetzliche Regelungen verstoßen, etwa gegen Datenschutzregelungen, wettbewerbsrechtliche Regelungen, gegen das Dienstrecht oder das Telemediengesetz (siehe Kapitel 5). Allen Landesbediensteten muss klar sein: Das Internet ist kein geschützter Raum, auch in vermeintlich abgegrenzten Nutzergruppen existiert mindestens eine Zugriffsmöglichkeit des Providers auf sämtliche dort bereitgestellten Daten. Ein Austausch über berufliche Zusammenhänge in internetgestützten Foren kann eine Verletzung von Betriebs- bzw. Amtsgeheimnissen darstellen und dienst- oder sogar strafrechtliche Folgen nach sich ziehen.

Rechtlich unbestritten ist die datenschutzrechtliche Verantwortung des Fanpage-Betreibers für die von ihm selbst auf der Seite veröffentlichten Informationen. Die Zulässigkeit der Veröffentlichung dieser Angaben bemisst sich nach den bereichsspezifischen Vorgaben, z.B. spezialgesetzliche Regelungen einschließlich dort geregelter Datenschutzbestimmungen, etwa im Gefahrenabwehrrecht, im Strafprozessrecht, im Umweltrecht, im Sozialrecht oder im Schulrecht.

Gleichzeitig ist zu beachten, dass sich die Anbieter von Social-Media-Plattformen in den Nutzungsbedingungen in der Regel die Rechte zur Verwendung der in Accounts und Fanpages eingestellten Daten einräumen lassen. Aus datenschutzrechtlicher Sicht handelt es sich daher bei einer solchen Veröffentlichung von Daten um eine Datenübermittlung. Hierfür fehlt es in den meisten Fällen an einer Rechtsgrundlage. Dies gilt insbesondere für Plattformbetreiber mit Sitz außerhalb der EU. Daher ist von der Veröffentlichung personenbezogener Daten in sozialen Medien abzusehen.

Auch die Veröffentlichung von anderen Informationen im Internet birgt besondere Risiken, weil das Internet mit speziellen Eigenschaften verbunden ist:

- **Kontrollverlust:** Bei einmal ins Netz gestellten Informationen muss damit gerechnet werden, dass diese dauerhaft oder zumindest über einen sehr langen Zeitraum im Netz verfügbar sind. Da die Informationen leicht kopiert und weltweit bereitgestellt werden können, ist eine Löschung unter Umständen sehr aufwendig oder sogar unmöglich – selbst wenn es eine rechtliche Handhabe zur Löschung gibt.

- **Durchsuchbarkeit:** U.a. durch die ständig aktiven, automatisiert arbeitenden Webcrawler, Suchmaschinen und Metasuchmaschinen werden die eingestellten Informationen schnell und mit komfortablen Suchmethoden gefunden und den weltweiten Nutzern zwar mittelbar aber bekanntlich sehr kurzfristig zugänglich gemacht.

- **Streuwirkung:** Im Internet verfügbare Informationen sind in der Regel einem nicht ab-

grenzbaren Adressatenkreis zugänglich. Durch die Datensammlung in verschiedenen Systemen, z.B. fachspezifischen Informationsplattformen, wird der Zugriff schnell gestreut.

- **Verknüpfbarkeit/Profilbildung:** Eingestellte Informationen können leicht mit Informationen zum selben Thema, zur selben Person oder zur selben Behörde verknüpft werden. Hierdurch werden unter Umständen wesentlich mehr Informationen preisgegeben, als beabsichtigt. Es können sogar Persönlichkeitsprofile gebildet werden (z.B. über Konsumverhalten, Bewegung und Nutzung des Internets), auf die die Betroffenen keine Einflussmöglichkeiten mehr haben. Auch besteht das Risiko, dass eigentlich anonymisierte oder pseudonymisierte Daten durch Verknüpfung zweier oder mehrerer Datenquellen mittels des Einsatzes von Data-Mining-, Datenanalyse- und Profilbildungssoftware wieder einen Personenbezug bekommen und so deren Bereitstellung das Datenschutzrecht verletzt. Auf diese Weise ist es auch möglich, dass eine Privatmeinung von Bediensteten einer Behörde zugeordnet wird.

- **Pflegeaufwand:** Damit einmal eingestellte Informationen korrekt bleiben, müssen sie bei Änderungen aktualisiert werden. Das Einstellen von Informationen erzeugt also einen oft nicht unerheblichen Folgeaufwand. Häufig wird auch erwartet, dass auf Fragen oder Kommentare sehr schnell geantwortet wird, was nicht immer leistbar ist. Möglicherweise ist eine „Pflege“ im Bereich der Social Media im Einzelfall gar nicht möglich, weil Nutzerinnen und Nutzer keine Zugriffsrechte für eine nachträgliche Änderung von eingestellten Informationen erhalten (z.B. in einem Blog).

Von besonderer Bedeutung sind Datenschutzrisiken in sozialen Netzwerken, denn Ziel mancher sozialer Netzwerke ist es, eine maximale Unterstützung bei der Knüpfung sozialer Kontakte zu erreichen, bei kommerziellem Geschäftsmodell zudem mit dem Ziel großer Reichweite für die erfolgreiche Generierung von Werbeeinnahmen. Dies führt bewusst gesteuert zu einer möglichst umfangreichen Verarbeitung personenbezogener Daten. Betroffene können sich dem nur mit erheblichem Aufwand durch Ausdifferenzierung in den Kontoeinstellungen entziehen. Sofern dort die Einstelloptionen nicht als Opt-in-Lösungen konzipiert sind oder deren Differenzierung nicht weitreichend genug ist, ist das Instrumentarium für den Selbstdatenschutz der Nutzer praktisch wirkungslos.

Auch wenn keine Daten eingestellt, sondern nur genutzt werden, können die besonderen Eigenschaften des Internets – besonders im Bereich der Social Media - zu hohen Risiken führen:

- **Unsichere Quellen:** Nicht alles, was schwarz auf weiß im Internet steht, ist korrekt. Es besteht die Gefahr, dass Datenquellen falsche oder minderwertige Informationen bereitstellen.

- **Unklare Quellenangaben:** Wenn man sich auf Quellen im Internet bezieht, so ist nicht gesichert, dass diese dauerhaft zur Verfügung stehen. In manchen Fällen ist es daher nicht ausreichend, sich auf diese Quellen zu beziehen.

- **Schadsoftware:** Natürlich besteht bei der Social-Media-Nutzung, so wie bei der Internetnutzung insgesamt, die Gefahr, dass hierdurch Schadsoftware den eigenen Rechner infiziert, z.B. durch das bedenkenlose Herunterladen und Ausführen von Programmen.

- **Datenpreisgabe:** Zum Teil sind Social-Media-Daten nur durch vorherige Registrierung zugänglich. Auch werden durch die Browser-Nutzung und durch die Speicherung von

Cookies Daten an die Anbieter übermittelt. Das Etablieren der Cookies auf dem Nutzerrechner geschieht häufig, ohne dass die Nutzer vorher eine gesetzlich geforderte[4] bewusste und eindeutige (ausdrückliche und informierte) Einwilligung gegeben haben. Nach EU-Recht[5] ist das Fehlen der Einwilligung ein Rechtsverstoß. Hierdurch kann es zu einer ungewollten Übermittlung personenbezogener Daten kommen. Facebook z.B. analysiert die Aktivitäten seiner Nutzerinnen und Nutzer hauptsächlich mit Hilfe von Cookies, die auf dem Rechner der Nutzerin oder des Nutzers abgelegt werden, und liefert Webseitenbetreibern aussagekräftige Nutzungsstatistiken und Reichweitenanalysen. Die Analyse beschränkt sich jedoch nicht auf die Nutzung von Facebook allein. Facebook kann auch nachvollziehen, welcher Nutzerin oder welcher Nutzer sich wie lange auf welcher Webseite aufgehalten hat. Durch die Auswertung des Nutzerverhaltens und des Userprofils ist Facebook in der Lage, zielgruppenorientierte Werbung zu platzieren.

5. Rechtliche Regelungen

Bei der Nutzung von Social Media, insbesondere bei der Veröffentlichung von Informationen, sind die einschlägigen gesetzlichen Regelungen zu beachten. Im Folgenden wird ein Überblick über die wichtigsten Regelungen gegeben.

5.1. Datenschutzrechtliche Regelungen

Bereitstellung von personenbezogenen Daten

Bei der Verarbeitung von personenbezogenen Daten durch Behörden und sonstige öffentliche Stellen Niedersachsens sind das Niedersächsische Datenschutzgesetz (NDSG) und weitere spezialgesetzliche Regelungen zu beachten (§ 2 NDSG). Diese Regelungen wirken sich natürlich auch auf die Social-Media-Nutzung aus. In diesem Zusammenhang ist besonders auf folgende Auszüge aus dem NDSG hinzuweisen:

- ***Zulässigkeit der Datenverarbeitung:*** *Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn das NDSG oder eine andere Rechtsvorschrift dies vorsieht oder die*

[4] § 13 Telemediengesetz

[5] Die so genannte „Cookie-Richtlinie“ oder auch E-Privacy-Richtlinie (Richtlinie 2002/58/EG, neu gefasst durch Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009, ABl. der EU, L 337/11; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:de:PDF) verlangt über § 15 Abs. 3 TMG hinausgehend in Art. 5 Abs. 3 beim Setzen von Cookies, die nicht allein für die Erbringung des Dienstes erforderlich sind und genutzt werden, die Einwilligung des Nutzers. Die Regelung wurde bislang zwar nicht in deutsches Recht umgesetzt, ist aber zwingend anzuwenden. Sie wird der Aufsichtspraxis in Deutschland daher zugrunde gelegt und kann von den Kontrollbehörden durchgesetzt werden.
Allgemein gilt für die Einholung von informierten Einwilligungen: Einwilligungen, die gemäß Art. 2 h, 7 a der Richtlinie 46/95/EG Grundlage für die Datenverarbeitung sein sollen, setzen eine vollständige, eindeutige und sprachlich angemessene Information der Nutzerinnen und Nutzer über die beabsichtigte Verwendung ihrer personenbezogener Daten und darauf bezogener Einfluss- bzw. Wahlmöglichkeiten voraus. Sie müssen ausdrücklich und eindeutig sein. Dies betrifft auch Einwilligungen in die Datenübermittlung an Anbieter von Applikationen („Apps“). Dazu zählen ebenfalls spezifische Informationen der Nutzerinnen und Nutzer über die Nutzung von „Apps“ von Anbietern, die in Ländern ohne ausreichendes Datenschutzniveau im Sinne der Richtlinie 95/46/EG belegen sind.

Betroffenen eingewilligt haben (§ 4 (1) NDSG).

- ***Datengeheimnis:*** *Den Personen, die bei öffentlichen Stellen oder ihren Auftragnehmern dienstlichen Zugang zu personenbezogenen Daten haben, ist es untersagt, diese zu einem anderen als dem zur jeweiligen Aufgabenerfüllung gehörenden Zweck zu verarbeiten oder zu offenbaren (§ 5 NDSG).*

- ***Datenübermittlung:*** *Die Übermittlung personenbezogener Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs ist gem. § 13 NDSG zulässig, wenn*

  1. *sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Daten nach § 10 NDSG verarbeitet werden dürfen,*

  2. *die Empfänger ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft machen und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Betroffenen an der Geheimhaltung überwiegt, oder*

  3. *sie im öffentlichen Interesse liegt oder hierfür ein berechtigtes Interesse geltend gemacht wird und die Betroffenen in diesen Fällen der Übermittlung nicht widersprochen haben.*

- ***Automatisiertes Abrufverfahren:*** *Ein automatisiertes Verfahren, das die Übermittlung personenbezogener Daten durch Abruf eines Dritten ermöglicht, darf nur eingerichtet werden, wenn eine Rechtsvorschrift dies zulässt. (…) Personenbezogene Daten dürfen nicht zum Abruf durch Personen oder Stellen außerhalb des öffentlichen Bereichs bereitgehalten werden. Dies gilt nicht für den Abruf durch Betroffene (§ 12 NDSG).*

Die Bereitstellung von personenbezogenen Daten in Social-Media-Angeboten der Verwaltung, auf die Personen außerhalb der Verwaltung zugreifen können, ist als Übermittlung, in besonderen Fällen auch als automatisiertes Abrufverfahren, anzusehen. In der Regel sind die Inhalte von Social Media – Angeboten weltweit verfügbar. Es erfolgt also auch eine Übermittlung ins außereuropäische Ausland, was die Zulässigkeit weiter einschränkt (§14 NDSG). Das NDSG erlaubt es somit der Verwaltung nur in Ausnahmefällen, personenbezogene Daten in Social-Media-Angeboten bereitzustellen.

Da viele Social-Media-Angebote nicht auf Servern in Deutschland bzw. im europäischen Wirtschaftsraum angeboten werden, stellt sich oft die Frage, welche Datenschutzregelungen die Anbieter einzuhalten haben. Die deutschen Datenschutzbehörden gehen davon aus, dass auch ausländische Unternehmen das Bundesdatenschutzgesetz (BDSG), landesrechtliche oder bereichsspezifische Regelungen zu beachten haben, wenn sie ihre Angebote in Deutschland bereitstellen.

Bei außereuropäischen Unternehmen, die Social-Media-Plattformen global und damit auch in Niedersachsen als Telemediendiensteanbieter zur Verfügung stellen, besteht mindestens die Gefahr, dass diese nicht die deutschen oder vergleichbare europäische Datenschutzregelungen einhalten. Nach Auffassung der deutschen Datenschutzbehörden ist dies trotz des Unternehmenssitzes außerhalb Europas gleichwohl erforderlich, da der Grundrechtsschutz hierzulande unterlaufen werden würde. Allerdings ist die Durchsetzbarkeit individueller und höchstpersönlicher Rechte – hier des Rechtes auf informationelle Selbstbestimmung in der Ausgestaltung der datenschutzrechtlichen Regelungen – praktisch sehr stark behindert. Den zuständigen Datenschutzaufsichtsbehörden in Deutschland stehen nur begrenzte Kontroll- und Sanktionsmöglichkeiten gegenüber den globalen Unternehmen zur Verfügung.

Veröffentlichung von Beschäftigtendaten im Internet

Auch für die Bereitstellung von personenbezogenen Daten der Beschäftigten in Social Media gelten die oben beschriebenen Regelungen. Nähere Einzelheiten hierzu ergeben sich aus der Bekanntmachung des Nds. Ministeriums für Inneres und Sport, der Nds. Staatskanzlei und der übrigen Ministerien vom 23.01.2012 (siehe Anhang 2). Danach dürfen Daten von Personen, deren Tätigkeit nach außen wirkt oder die eingewilligt haben, im Internet veröffentlicht werden. Darüber hinaus ist die Veröffentlichung im Einzelfall möglich, wenn dies aus dienstlichen Gründen erforderlich ist. Betroffene können wegen überwiegender schutzwürdiger Belange der Veröffentlichung widersprechen.

Datenschutzaspekte bei Angeboten ohne personenbezogene Inhaltsdaten

Auch wenn in den Social-Media-Angeboten der Verwaltung keine personenbezogenen Inhaltsdaten eingestellt werden, können Datenschutzregelungen von Bedeutung sein. Die besonderen Social-Media-Kommunikationsformen führen nämlich dazu, dass Nutzerinnen und Nutzer bewusst und unbewusst Daten bereitstellen, die auf ihre Person bezogen werden können. Dies beginnt mit der Übermittlung von IP-Adressen, die allerdings nur unter bestimmten Rahmenbedingungen[6] einer Person zugeordnet werden können. Außerdem erfolgt durch Social-Media-Angebote häufig ein Zugriff auf Cookies, die auf dem Rechner der Nutzerin oder des Nutzers gespeichert sind. Bei der Nutzung von Suchmaschinen kann der Suchbegriff ausgewertet werden. Es hängt von der Social Media – Ausprägung ab, ob in diesen Fällen Daten ausschließlich an den Social Media – Anbieter übermittelt werden oder auch an die Behörde, die einen Behördenauftritt eingestellt hat. Falls eine Behörde zweites vorsieht, ist von ihr die Rechtmäßigkeit der Datenverarbeitung, insbesondere das Vorhandensein einer Rechtsgrundlage, zu prüfen und ggf. die Nutzung der übermittelten Daten in der Behörde rechtskonform zu gestalten. So richtet sich die Zulässigkeit der Verarbeitung von IP-Adressen nach dem Telemediengesetz.

5.2. Pflichten für Diensteanbieter von Telemedien

Telemedien sind nach § 1 Abs. 1 Telemediengesetz (TMG) alle elektronischen Informations- und Kommunikationsdienste, die weder Rundfunk noch reine Telekommunikationsdienste oder telekommunikationsgestützte Dienste sind. Hierzu gehören nach Auffassung des Landesbeauftragten für den Datenschutz auch Online-Dienste wie www-Angebote. Diensteanbieter von Telemedien müssen u.a. beachten[7]:

- Impressumspflicht[8]

---

[6] Eine direkte Zuordnung der IP-Adresse zu einer Person ist nur dem Provider möglich, der für den Nutzer den Internetzugang herstellt. Der Provider kann den Kunden benennen, der den Providervertrag eingegangen ist, nicht die Person, die tatsächlich den Rechner nutzt. Wenn lokale Netzwerke verwendet werden, muss auch dort die IP-Adresse zugeordnet werden können. Da IP-Adressen in der Regel dynamisch, d.h. für jede Sitzung vom Provider neu vergeben werden, muss auch Datum und Uhrzeit bekannt sein, um eine Zuordnung vornehmen zu können. Der Provider muss diese Daten (noch) gespeichert haben.

[7] Nähere Informationen in der „Orientierungshilfe für Telemedien“ des Landesbeauftragen für den Datenschutz Niedersachsen“, siehe: www.lfd.niedersachsen.de

[8] Ob für Facebook-Profile, Fanpages oder Twitteraccounts ein Impressum erforderlich ist oder nicht, ist gerichtlich bisher nicht entschieden. Die maßgeblichen Regelungen, § 5 Telemediengesetz (TMG) bzw. § 55

- Vermeidung von Links mit rechtswidrigen Inhalten
- Datenschutzgerechter Umgang mit personenbezogenen Daten
- Unterrichtung vor Nutzung bzw. Einwilligung vor Verarbeitung von personenbezogenen Daten
- Einwilligung vor Erstellung von Nutzungsprofilen
- Versand von Newslettern in der Regel nur mit Einwilligung. Beachtung des Rechts auf Widerruf.

5.3. Personalvertretungsgesetz

Die Einbindung von Social-Media-Angeboten in die Arbeitsabläufe der Verwaltung kann zu einer Mitbestimmungspflicht nach § 67 des Niedersächsischen Personalvertretungsgesetzes (NPersVG) führen. Der Personalrat bestimmt u.a. bei folgenden Maßnahmen mit:

- Einführung und Anwendung technischer Einrichtungen, die geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen,
- Maßnahmen zur Hebung der Arbeitsleistung und zur Erleichterung des Arbeitsablaufs,
- Einführung grundlegend neuer Arbeitsmethoden.

Das Mitbestimmungsverfahren ist in § 68ff NPersVG geregelt und ggf. Voraussetzung für die Einbindung von Social Media in die Arbeitsabläufe.

5.4. Dienstrecht

Bei der dienstlichen Nutzung von Social-Media-Angeboten sind beamten- und arbeitsrechtliche Vorschriften (z.B. NBG, BeamtStG, TV-L) zu beachten.

Hervorzuheben sind hierbei insbesondere:

- Verschwiegenheitspflicht (§ 37 BeamtStG, § 3 Abs. 2 TV-L),
- Pflicht zu achtungs- und vertrauenswürdigem Verhalten (§ 34 Satz 3 BeamtStG)
- Mäßigung bei politischer Tätigkeit (§ 33 Abs. 2 BeamtStG).

Wichtig ist, dass diese Vorschriften zum Teil auch bei der privaten Nutzung von Social-Media-Angeboten zu berücksichtigen sind.

Rundfunkstaatsvertrag (RStV) sprechen ausweislich des Wortlauts gerade nicht nur von Webseiten, sondern ausdrücklich von Telemedien. Dies dient nach dem Willen des Gesetzgebers gerade auch dazu neue, im Zeitpunkt der Gesetzgebung noch nicht bekannte Dienste einzuschließen.

5.5. Urheberrechtliche und wettbewerbsrechtliche Regelungen

Bei der Veröffentlichung von Daten können Urheberrechte, Titelschutzrechte, Marken-, Kennzeichen- oder sonstigen Namensrechte verletzt werden. Dies kann bei Behördenauftritten in Social Media von erheblicher Bedeutung sein. Fotografien sind urheberrechtlich geschützt (§ 72 UrhG). Z.B. ist vor der Einstellung von Fotos von Bediensteten deren schriftliche Einwilligung einzuholen (siehe Anhang 2). Auch Dokumente oder Computerprogramme aus dem Internet sind urheberrechtlich geschützt. Ebenso können bei der Veröffentlichung von neuen Begriffen (z.B. für ein Projekt), Icons oder Logos leicht Rechte verletzt werden. Die Social-Media-Nutzung darf nicht zur Verletzung dieser Rechte führen. Ggf. ist Zurückhaltung geboten.

6. Organisatorische Regelungen

Neben den rechtlichen Regelungen müssen auch organisatorische Regelungen wie Dienstanweisungen bei der Nutzung von Social Media beachtet werden. Von Bedeutung ist z.B. die „Rahmendienstanweisung für die Nutzung des vom (damaligen) IZN betriebenen Internetzugangs der Landesverwaltung“. In ihr ist u.a. Folgendes geregelt:

- Das Internet darf nur zu dienstlichen Zwecken genutzt werden.
- Daten der Schutzstufe C und D dürfen nicht unverschlüsselt über das Internet übertragen werden, es sei denn die Betroffenen haben zugestimmt. Daten der Schutzstufe E dürfen in angeschlossenen lokalen Netzen nicht verarbeitet werden.

7. Verhaltensregeln für Social Media

Aus den geschilderten Risiken und den aufgeführten rechtlichen und organisatorischen Regelungen ergibt sich, dass die Nutzung von Social Media durch die Verwaltung nur unter Beachtung der folgenden Verhaltensregelungen erfolgen soll. Dabei wird unterschieden zwischen Regeln für die Nutzung von Angeboten durch Bedienstete und der Bereitstellung von Behördenauftritten in Social-Media-Angeboten.

7.1. Verhaltensregeln für die Nutzung von Social Media durch Bedienstete

1. **Seriöse Datenquellen:** Nur wenn die Social-Media-Nutzung ohne Preisgabe sensibler Daten möglich ist, ist sie unbedenklich. Die datenschutzrechtlichen Vorgaben zur Verarbeitung personenbezogener Daten sind auch hier zu beachten (vgl. Ziffer 5.1). Bei der Verwendung der beschafften Daten ist auf deren Seriosität zu achten. Wichtige Entscheidungen dürfen nur auf der Grundlage verlässlicher Quellen getroffen werden. Es ist auf eine korrekte Quellenangabe zu achten. Im Rahmen der Sichtung von Presseartikeln mit Behördenrelevanz sollte das Internet einschließlich wichtiger sozialer Medien mit einbezogen werden. Fachbereiche sollten die für Öffentlichkeitsarbeit zuständige Stelle über

wichtige Veröffentlichungen im Internet informieren.

2. **Anonyme oder pseudonyme Nutzung:** Ist für die Social-Media-Nutzung eine Nutzerregistrierung erforderlich, ist zu prüfen, ob durch die Verwendung von Pseudonymen eine Preisgabe von sensiblen Daten verhindert werden kann. Bereits Name und Zugehörigkeit zu einer Behörde können sensible Daten sein, z.B. wenn kritische persönliche Äußerungen als offizielle Äußerungen der Behörde gewertet werden.

3. **Personenbezogene Nutzung erfordert Freigabe:** Die personenbezogene Social-Media-Nutzung für Fachleute, z.B. im Rahmen von fachbezogenen Foren mit Kolleginnen und Kollegen, sollte von der Organisationsleitung der Behörde geprüft werden. Eine Nutzungsfreigabe sollte nur erfolgen, wenn die in diesem Leitfaden aufgeführten Eckpunkte beachtet werden können. Die Fachleute müssen bei ihren Äußerungen darauf achten, dass sie behördenbezogene Äußerungen vornehmen. Innerhalb einer Behörde sollten für den fachlichen Austausch grundsätzlich intranetgestützte Angebote Vorrang haben.

4. **Privat und dienstlich trennen:** Eine private Nutzung sozialer Medien soll im Dienst nicht erfolgen (Verbot der Internetnutzung für private Zwecke). Bei der privaten Nutzung außerhalb des Dienstes ist darauf zu achten, dass keine dienstlichen Äußerungen erfolgen. Bedienstete dürfen im privaten Bereich mit ihrem Namen und ihrem Bild an Social Media – Angeboten teilnehmen,[9] sollten aber berücksichtigen, dass dies ihre beruflichen Verwendungsmöglichkeiten im Landesdienst einschränken kann. Insbesondere für Angehörige von Sicherheitsbehörden weist die Nutzung von Sozialen Netzwerken mit Profilfotos erhebliche Risiken auf, da durch biometrische Software bereits heute eine Gesichtskennung möglich ist und das Foto mit persönlichen Daten verknüpft werden kann. Es wird empfohlen, bei Berufsangaben keine oder nur allgemeine Angaben („öffentlicher Dienst“) zu machen. Auf diese Weise wird auch verhindert, dass persönliche Meinungsäußerungen als Stellungnahmen der Behörde verstanden werden. Bei Äußerungen ist auf das Mäßigungsgebot zu achten (§ 33 BeamtStG).

5. **Ggf. Schulung anbieten:** Wenn die Nutzung von Social Media für die dienstliche Aufgabenerledigung erforderlich ist und ein vertieftes Wissen erfordert, sind den Bediensteten geeignete Schulungen anzubieten.

6. **Sichere Datenübermittlung:** Schützenswerte Dateneingaben sollten nur mit SSL-Verschlüsselung (per https) übertragen werden, um unbefugtes Mitlesen zu verhindern. Hierfür müssen die Anbietenden ihre Internetseite entsprechend eingerichtet haben. Dies ist der Fall, wenn die Internetadresse mit „https“ beginnt bzw. der Internetbrowser anzeigt, dass die Übertragung verschlüsselt erfolgt.

7. **Berücksichtigung von bestehenden Dienstanweisungen:** Bereits bestehende Dienstanweisungen, z.B. zur dienstlichen Nutzung des Internets, sind zu beachten.

[9] Ein Verbot der privaten Nutzung ist in bestimmten Verwaltungsbereichen möglich, z.B. wenn hierdurch bei der Polizei Fahndungserfolge oder Kollegen gefährdet werden. Die Verbote sollten dort dann speziell geregelt werden.

7.2. Verhaltensregeln für die Behördenauftritte in Social Media

1. **Erforderlichkeit:** Vor der Nutzung von Social Media ist zunächst zu prüfen, ob diese zur Aufgabenerfüllung geeignet sind. Ist eine Aufgabe auf weniger risikobehaftetem Wege genauso effektiv bzw. effizient erfüllbar, sollte sie unterbleiben.

2. **Rechtmäßigkeit von Social-Media-Angeboten:** Vor der Erstellung von Behördenauftritten bei Social-Media-Anbietern ist zu prüfen, ob diese Datenschutzregelungen im ausreichenden Maß berücksichtigen. Besonders zu beachten ist dies bei außereuropäischen Anbietern, weil diese die deutschen Datenschutzregelungen einzuhalten, die zuständigen Aufsichtsbehörden aber keine Prüf- und Sanktionsmöglichleiten haben. In diesen Fällen ist nach Lösungsmöglichkeiten zu suchen, die den datenschutzrechtlichen Anforderungen entsprechen. Dazu bedarf es auch klarer Kompetenzregelungen.

3. **Keine Veröffentlichung personenbezogener Daten:** Grundsätzlich ist von der Veröffentlichung personenbezogener Daten in Social-Media-Auftritten von Behörden abzusehen. Die wirksame Vereinbarung einer Auftragsdatenverwaltung mit dem Plattformbetreiber, die eine wesentliche Voraussetzung für die rechtmäßige Datenübermittlung an diesen wäre, ist in der Regel nicht möglich.

4. **Rechtliche Regelungen beachten:** Neben dem Datenschutzrecht müssen bei Behördenpräsenzen in Web 2.0 – Verfahren insbesondere folgende rechtliche Regelungen eingehalten werden:

   - Telemediengesetz (TMG), z.B. Impressumspflicht
   - Urheberrechtliche und wettbewerbsrechtliche Regelungen
   - Dienstrechtliche Regelungen
   - Personalvertretungsgesetz

   Genauere Informationen hierzu sind in Kapitel 5 aufgeführt.

5. **Kontrolle behalten:** Wenn im Rahmen der Optimierung Social Media in die dienstliche Aufgabenerledigung mit einbezogen werden, sind Rahmenbedingungen zu schaffen, um die Kontrolle über die Aufgabenerledigung zu behalten. Z.B. ist auf Folgendes zu achten:

   - Manipulationen müssen verhindert werden. Z.B. muss sichergestellt sein, dass auf Präsentationen der Behörde keine Unbefugten schreibend zugreifen können.
   - Der Social-Media-Dienst muss dauerhaft zur Verfügung stehen.
   - Es muss weiterhin eine vollständige, transparente Aktenführung gewährleistet sein[10].
   - Die für geschlossene Benutzergruppen bereitgestellten Daten dürfen nur Befugten zugänglich sein.
   - Die Unterstützung durch den Social-Media-Dienst sollte durch eine andere Unterstützung ersetzbar sein.

   Insbesondere wenn sensible Daten (z.B. Personaldaten, Unterlagen in Vergabeverfahren) durch einen Diensteanbieter im Internet verarbeitet werden sollen, muss die Behörde als Auftraggeber durch klare, ggf. individuelle vertragliche Regelungen mit dem Anbieter für eine rechtlich einwandfreie Datenverarbeitung sorgen. Wenn Social-Media-Dienste solche

[10] Aktenrelevante Daten dürfen daher nicht ausschließlich in Social-Media-Angeboten gespeichert werden, sondern sind nach der Nds. Aktenordnung aufzubewahren.

Regelungen nicht akzeptieren, muss die Verarbeitung unterbleiben.

6. **Bedienstete schützen:** Bei Behördenauftritten ist auch der Schutz der Privatsphäre von Bediensteten zu berücksichtigen. Diese dürfen nicht dazu gezwungen werden, eigene oder andere personenbezogene Daten in sozialen Medien preiszugeben. Soweit Kennungen bereitgestellt werden müssen, sind Funktionskennungen zu verwenden. Die Pflichten zur Beteiligung des Personalrats sind zu beachten.

7. **Geschlossene Benutzergruppen:** Wenn Social Media nur von Bediensteten der Verwaltung genutzt werden sollen, sollten interne Angebote verwendet werden. Intranet-Präsentationen, Community-Plattformen, Foren oder Wikis können z.B. mithilfe des Content-Management-Systems des Landesintranets betrieben werden. Kollaborations- und eAkte-Systeme stellt der LSKN auf Anforderung gegen Entgelt bereit.

8. **Geschäftsbedingungen beachten:** Vor der Einrichtung eines Behördenauftritts sind die Geschäftsbedingungen des Social-Media-Anbieters genau zu prüfen. Besondere Vorsicht ist geboten, wenn Social-Media-Anbieter sich vorbehalten, die Allgemeinen Geschäftsbedingungen ohne Zustimmung der Nutzerinnen und Nutzer zu ändern.

9. **Nutzerinnen und Nutzer über Risiken informieren:** Nutzerinnen und Nutzer müssen über Risiken informiert werden, die sie bei Nutzung eines Behördenauftritts eingehen. Dies gilt insbesondere, wenn die Einwilligung der Betroffenen eingeholt werden muss („informierte Einwilligung“). Die wichtigsten Hinweise betreffen folgende Punkte:

   - Kontaktdaten der für die Datenverarbeitung verantwortlichen Stelle.
   - Zweck und Umfang der Datenverarbeitung und Verbleib der personenbezogenen Daten.
   - Eingaben, die nicht veröffentlicht werden, möglichst per SSL-Verschlüsselung (https) versenden, um unbefugtes Mitlesen zu verhindern.

   Wenn die Nutzung mit erheblichen Risiken verbunden ist, muss es alternative Informations- bzw. Beteiligungsangebote geben. Wenn Nutzerinnen und Nutzer sensible personenbezogene oder sicherheitsrelevante Daten übermitteln und hierauf eine Antwort erwarten, sollten diese so beantwortet werden, dass diese gegen Zugriff geschützt übermittelt werden. Ist dies nicht möglich, ist auf eine Übermittlung zu verzichten.

10. **Behördenpräsentation erfordert Freigabe:** Ist vorgesehen, die Behörde oder Teile von ihr in den Social Media zu präsentieren, so ist vorher die Stelle für Öffentlichkeitsarbeit zu beteiligen[11]. Diese Stelle hat die Freigabe der Präsentation zu erteilen. Abhängig von der Art der Präsentation sollte diese Freigabe einmalig mit dauerhafter Gültigkeit oder für jede Änderung eingeholt werden. Presseinformationsähnliche Veröffentlichungen sollten immer von der für Öffentlichkeitsarbeit zuständigen Stelle freigegeben werden.

11. **Social-Media-Netiquette beachten**: Beim Umgang mit Social Media sollten Behörden auf den passenden Umgangsstil achten. Z.B. sollten folgende Punkte beachtet werden:

    - Allgemeinverständliche, kurze Texte verwenden!
    - Auf dienstlichen Charakter hinweisen!

[11] Die Behörden können hiervon abweichende Regelungen treffen.

- Sachlich und korrekt, nicht verletzend formulieren!
- Formulierungen adressatengerecht, aber in amtlicher deutscher Rechtschreibung!
- Nicht abgestimmte Auffassungen als solche kennzeichnen!
- Quellen, Urheber angeben!

12. **Missbrauch von Behördenidentitäten**: Verwenden Nutzerinnen und Nutzer Behördenidentitäten missbräuchlich (z.B. wenn fremde Personen sich als Sprecher einer Behörde ausgeben), sind verschiedene Gegenmaßnahmen denkbar. Sie richten sich nach dem Schadensausmaß des Missbrauchs und den Möglichkeiten, den Missbrauch einzuschränken. Ggf. sind der entsprechende Nutzer oder die Nutzerin, der Dienstanbieter oder die zuständige Polizeibehörde auf den Missbrauch hinzuweisen. Sichern Sie hierzu die Kommunikationsdaten, um den Missbrauch deutlich zu machen.

13. **Umgang mit Social Plug-ins**: Über soziale Erweiterungsmodule (englisch „Social Plug-ins“) können Website-Betreiber einfach kleine Anwendungen mit minimalem Programmieraufwand im eigenen Portal integrieren. Die beliebtesten Plug-ins sind der *Like Button*, die *Like Box* und die *Facebook Comment Box.* Der IT-Planungsrat[12] des Bundes und der Länder empfiehlt, von der direkten Einbindung von Social Plug-ins ohne Einwilligungsmöglichkeit abzusehen. Wenn Behördenseiten dennoch Links zu Social Media enthalten sollen, müssen daher die Nutzer vor einer Übertragung von Daten ausreichend informiert werden. Hierfür ist eine konkrete Information über Art und Umfang der Datenverarbeitung erforderlich. Dies kann beispielsweise mit dem folgenden Textbaustein erfolgen:

    - Durch Anklicken dieses Links werden bestimmte Daten, die Ihr Internet-Browser speichert, für xyz verfügbar. Hierzu gehören die IP-Adresse, die aktuelle URL sowie Cookies, die xyz in früheren Sessions auf Ihrem Rechner abgespeichert wurden. Sie müssen damit rechnen, dass xyz diese Daten abruft, Ihrem Account zuordnet und auswertet. Verwenden Sie diesen Link nur, wenn Sie mit dieser Datenverarbeitung einverstanden sind.

    Im Internet werden Lösungen[13] beschrieben, wie an sich unzureichende Social Plug-ins mithilfe von vorgeschalteten „Aktivierungs-Buttons“ so eingesetzt werden können, dass die datenschutzrechtlichen Anforderungen erfüllt werden.

[12] Beschluss des IT-Planungsrat vom 8.03.2012, TOP 17
[13] Z. B. http://www.heise.de/ct/artikel/2-Klicks-fuer-mehr-Datenschutz-1333879.html

Herausgeber:

Niedersächsisches Ministerium für Inneres und Sport, Lavesallee 6, 30165 Hannover

Internet: www.mi.niedersachsen.de

Quellen:

1. Social Media Guidelines – Web 2.0 in der deutschen Verwaltung, Dr. Sönke E. Schulz, ISPRAT, 2011

2. Social Media in der Hamburgischen Verwaltung – Hinweise, Rahmenbedingungen und Beispiele, Freie und Hansestadt Hamburg, Finanzbehörde, Version 1.1, 2011

Anhang 1: Web 2.0 – Ausprägungen

Im Folgenden sind typische Web 2.0-Ausprägungen aufgelistet und kurz erläutert. Die Liste ist nicht abschließend.

Soziale Netzwerke
Stellen soziale Beziehungen im Internet dar. Sie ermöglichen es Nutzerinnen und Nutzern ein Profil zu erstellen und Kontakte zu verwalten. Meist können sich die Mitglieder in Gruppen oder Communities untereinander austauschen.
Beispiele: Facebook[14], myspace, Xing

Wikis:
Eine Ansammlung von Webseiten, die von Benutzerinnen und Benutzern frei erstellt und überarbeitet werden können.

Weblogs (Blogs):
Werden oftmals als Tagebuch im Internet bezeichnet. Ein festgelegter Autorenkreis verfasst Einträge, die in chronologisch umgekehrter Reihenfolge aufgelistet werden. Der Leser oder die Leserin kann Kommentare zu den Einträgen verfassen.

Mikrobloggings:
Blogs, bei der die Benutzer kurze, SMS-ähnliche Textnachrichten veröffentlichen können.
Beispiel: Twitter

Foren:
Virtueller Platz zum Austausch und Archivierung von Gedanken, Meinungen und Erfahrungen. Die Kommunikation findet dabei asynchron, das heißt nicht in Echtzeit, statt.

Newsgroups:
Virtuelle Internetforen, in denen zu einem umgrenzten Themenbereich Textbeiträge ausgetauscht werden. Veröffentlicht ein Benutzer oder eine Benutzerin einen Artikel in einer Newsgroup, so wird dieser an einen Newsserver gesendet. Dieser kann den Artikel dann seinen Benutzerinnen und Benutzern zur Verfügung stellen und an andere Server weiterleiten, die ihn wiederum ihren Benutzenden zur Verfügung stellen.

Podcasts:
Bezeichnet eine Veröffentlichungsform von Audio- und Videodateien im Internet. Sie können mit einfachen Mitteln eingestellt und mithilfe von Feedreadern bzw. Podcatchern von überall abgerufen werden.

Media-Sharing-Plattformen:
Interessierten Benutzerinnen und Benutzern bieten die Plattformen die Möglichkeit ein Profil anzulegen, Mediendaten wie Fotos, Audiodateien und Videos zu speichern und Inhalte anderer Nutzer zu konsumieren sowie zu bewerten.
Beispiel: youtube, flickr

Document-/Content-Plattformen:
Plattformen, auf die Nutzer oder Nutzerinnen beliebige Daten hochladen können und so als

[14] Laut SocialMedia Schweiz hatte Facebook im Mai 2011 689 Mio. Nutzerinnen und Nutzer, davon 19 Mio. in Deutschland (ca. 1/3 der Internet-Nutzerinnen und -Nutzer)

Speicherbereich im Internet mit anderen Nutzern zusammen verwenden können.
Beispiel: GoogleDocs

Virtuelle Welten:
Online-Angebote, in denen Nutzer oder Nutzerinnen über das Internet als virtuelle Personen (Avatar) an einer Computeranimation teilnehmen können, die einer realen Welt nachempfunden ist. In virtuellen Welten können sich mehrere Nutzer gleichzeitig anmelden, sich unabhängig voneinander im virtuellen Raum bewegen und miteinander kommunizieren.
Beispiel: Second Life

Online-Spiele
Computerspiele, die über das Internet mit anderen Nutzerinnen und Nutzern gespielt werden können.

Anhang 2:
Bekanntmachung „Veröffentlichung von Beschäftigtendaten im Internet“[15]

Mit der zunehmenden Kommunikation über das Internet präsentieren sich die meisten Landesbehörden auf einer eigenen Homepage im Internet. Dabei werden in der Regel auch Daten der Beschäftigten aufgeführt. Zur Veröffentlichung personenbezogener Daten der Beschäftigten der Behörden werden die folgenden Hinweise gegeben:

1. Die Veröffentlichung von Beschäftigtendaten im Internet ist insbesondere dann zulässig, wenn

1.1 die Betroffenen eingewilligt haben (§ 4 NDSG) oder

1.2 diese zur Durchführung organisatorischer Maßnahmen erforderlich ist (§ 88 Abs. 1 NBG bzw. § 13 Abs. 1 Nr. 1 i.V.m. § 10 NDSG für nicht beamtete Beschäftigte).

2. Als erforderlich (s. Nummer 1.2) wird die Veröffentlichung personenbezogener Daten (s. Nummer 1) angesehen bei Personen, deren Tätigkeit nach außen wirkt (z.B. Pressesprecherinnen und Pressesprecher, Angehörige der Behördenleitung, Beauftragte der LReg, Ansprechpartnerinnen und Ansprechpartner für Projekte mit Bürgerbeteiligung). Diese Auffassung wird bestätigt durch den Beschl. des BVerwG 2 B 131.07 vom 12.8.2008, nach dem Behörden im Rahmen ihres organisatorischen Ermessens auch ohne ausdrückliche gesetzliche Ermächtigung befugt sind, außenstehenden Benutzern einen Hinweis auf die zuständigen Personen (Beschäftigte) zu geben.

3. Zu den in Nummer 2 genannten Personen dürfen veröffentlicht werden:

- Name, Vorname
- Tätigkeitsbereich (Behördenbezeichnung, Organisationseinheit)
- Adresse der Dienststelle
- dienstliche Telefonnummer, dienstliche Telefaxnummer
- dienstliche E-Mail – Adresse.

Die Einstellung von Fotos im Internet bedarf der schriftlichen Einwilligung der Beschäftigten (§§ 22 ff. des Gesetzes betreffend das Urheberrecht an Werken der bildenden Künste und der Fotografie).

4. Sofern personenbezogene Daten von weiteren Beschäftigten(gruppen) veröffentlicht werden sollen, ist im Einzelfall abzuwägen, ob dies dienstlich tatsächlich erforderlich ist. Im Hinblick auf die vielfältigen Möglichkeiten der modernen Informations- und Kommunikationstechniken bei der Verarbeitung personenbezogener Daten und die damit verbundenen Risiken (z.B. Verknüpfung und Bildung von Persönlichkeitsprofilen) sollten auch Alternativen erwogen werden wie „neutrale“ Referats- bzw. Funktionspostfächer (anstelle von persönlichen E-Mail-Adressen) oder Referatsanschriften. Bei Internetangeboten, die eine Kontaktaufnahme mit der Behörde ermöglichen sollen, wird dies in der Regel ausreichend sein.

[15]Gem. Bek. D. MI, d. StK u. d. übr. Min. v. 23.1.2012 – 43.36-05419/010 - Nds. MinBl. Nr. 4/2011 S.114

5. Um die Entscheidung der Dienststelle über die Veröffentlichung personenbezogener Daten einzelner Beschäftigter nachvollziehbar festzuhalten, ist sie aktenkundig zu machen. Die betroffenen Beschäftigten sind von der beabsichtigten Veröffentlichung rechtzeitig in Kenntnis zu setzen. Wenn Betroffene wegen überwiegender schutzwürdiger Belange der Veröffentlichung widersprechen, hat sie zu unterbleiben.

Anhang 3: Behörden-Leitfaden für Bedienstete:
Umgang mit webbasierten sozialen Medien (Social Media)

Im Internet gibt es eine große Anzahl verschiedener Social-Media-Ausprägungen. Typische Ausprägungen sind soziale Netzwerke, Wikis, Blogs, Foren oder Newsgroups. Zur Zeit der Erstellung dieses Leitfadens sind z.B. das soziale Netzwerk Facebook, der Mikroblogging-Dienst Twitter und das Wiki Wikipedia besonders häufig frequentierte Social-Media-Angebote. Die Nutzung von Social Media bietet für die öffentliche Verwaltung interessante Chancen zur Verbesserung der Arbeitserledigung. Eine wachsende Anzahl von Behörden, sowohl in Kommunal- als auch in Landesverwaltungen nutzt diese zusätzlich zur vorhandenen Internetrepräsentanz. Sie birgt aber auch zahlreiche Risiken. Die Nutzung von Social Media durch die Verwaltung sollte daher nur unter Beachtung der folgenden Verhaltensregelungen erfolgen. Dabei wird unterschieden zwischen Regeln für die Nutzung von Angeboten durch Bedienstete und der Bereitstellung von Behördenauftritten in Social-Media-Angeboten.

Verhaltensregeln für die Nutzung von Social Media durch Bedienstete

1. **Seriöse Datenquellen:** Nur wenn die Social-Media-Nutzung ohne Preisgabe sensibler Daten möglich ist, ist sie unbedenklich. Die datenschutzrechtlichen Vorgaben zur Verarbeitung personenbezogener Daten sind auch hier zu beachten. Bei der Verwendung der beschafften Daten ist auf deren Seriosität zu achten. Wichtige Entscheidungen dürfen nur auf der Grundlage verlässlicher Quellen getroffen werden. Es ist auf eine korrekte Quellenangabe zu achten. Im Rahmen der Sichtung von Presseartikeln mit Behördenrelevanz sollte das Internet einschließlich wichtiger sozialer Medien mit einbezogen werden. Fachbereiche sollten die für Öffentlichkeitsarbeit zuständige Stelle über wichtige Veröffentlichungen im Internet informieren.

2. **Anonyme oder pseudonyme Nutzung:** Ist für die Social-Media-Nutzung eine Nutzerregistrierung erforderlich, ist zu prüfen, ob durch die Verwendung von Pseudonymen eine Preisgabe von sensiblen Daten verhindert werden kann. Bereits Name und Zugehörigkeit zu einer Behörde können sensible Daten sein, z.B. wenn kritische persönliche Äußerungen als offizielle Äußerungen der Behörde gewertet werden.

3. **Personenbezogene Nutzung erfordert Freigabe:** Die personenbezogene Social-Media-Nutzung für Fachleute, z.B. im Rahmen von fachbezogenen Foren mit Kolleginnen und Kollegen, sollte von der Organisationsleitung der Behörde geprüft werden. Eine Nutzungsfreigabe sollte nur erfolgen, wenn die in diesem Leitfaden aufgeführten Eckpunkte beachtet werden können. Die Fachleute müssen bei ihren Äußerungen darauf achten, dass sie behördenbezogene Äußerungen vornehmen. Innerhalb einer Behörde sollten für den fachlichen Austausch grundsätzlich intranetgestützte Angebote Vorrang haben.

4. **Privat und dienstlich trennen:** Eine private Nutzung sozialer Medien soll im Dienst nicht erfolgen (Verbot der Internetnutzung für private Zwecke). Bei der privaten Nutzung außerhalb des Dienstes ist darauf zu achten, dass keine dienstlichen Äußerungen erfolgen. Bedienstete dürfen im privaten Bereich mit ihrem Namen und ihrem Bild an Social-Media-Angeboten teilnehmen, sollten aber berücksichtigen, dass dies ihre beruflichen Verwen-

dungsmöglichkeiten im Landesdienst einschränken kann[16]. Insbesondere für Angehörige von Sicherheitsbehörden weist die Nutzung von Sozialen Netzwerken mit Profilfotos erhebliche Risiken auf, da durch biometrische Software bereits heute eine Gesichtskennung möglich ist und das Foto mit persönlichen Daten verknüpft werden kann. Es wird empfohlen, bei Berufsangaben keine oder nur allgemeine Angaben („öffentlicher Dienst") zu machen. Auf diese Weise wird auch verhindert, dass persönliche Meinungsäußerungen als Stellungnahmen der Behörde verstanden werden. Bei Äußerungen ist auf das Mäßigungsgebot zu achten (§ 33 BeamtStG).

5. **Ggf. Schulung wahrnehmen:** Wenn die Nutzung von Social Media für die dienstliche Aufgabenerledigung erforderlich ist und ein vertieftes Wissen erfordert, sollten Bedienstete geeignete Schulungen wahrnehmen (extern, solange landesintern kein entsprechendes Angebot besteht).

6. **Sichere Datenübermittlung:** Schützenswerte Dateneingaben sollten nur mit SSL-Verschlüsselung (per https) übertragen werden, um unbefugtes Mitlesen zu verhindern. Hierfür müssen die Anbietenden ihre Internetseite entsprechend eingerichtet haben. Dies ist der Fall, wenn die Internetadresse mit „https" beginnt bzw. der Internetbrowser anzeigt, dass die Übertragung verschlüsselt erfolgt.

7. **Berücksichtigung von bestehenden Dienstanweisungen:** Bereits bestehende Dienstanweisungen, z.B. zur dienstlichen Nutzung des Internets, sind zu beachten.

Verhaltensregeln für die Behördenauftritte in Social Media

8. **Erforderlichkeit:** Vor der Nutzung von Social Media ist zunächst zu prüfen, ob diese zur Aufgabenerfüllung geeignet sind. Ist eine Aufgabe auf weniger risikobehaftetem Wege genauso effektiv bzw. effizient erfüllbar, sollte sie unterbleiben.

9. **Rechtmäßigkeit von Social-Media-Angeboten:** Vor der Erstellung von Behördenauftritten bei Social-Media-Anbietern ist zu prüfen, ob diese Datenschutzregelungen im ausreichenden Maß berücksichtigen. Besonders zu beachten ist dies bei außereuropäischen Anbietern, weil diese die deutschen Datenschutzregelungen einzuhalten, die zuständigen Aufsichtsbehörden aber keine Prüf- und Sanktionsmöglichleiten haben. In diesen Fällen ist nach Lösungsmöglichkeiten zu suchen, die den datenschutzrechtlichen Anforderungen entsprechen. Dazu bedarf es auch klarer Kompetenzregelungen.

10. **Rechtliche Regelungen beachten:** Neben dem Datenschutzrecht müssen bei Behördenpräsenzen in Web 2.0 – Verfahren insbesondere folgende rechtliche Regelungen eingehalten werden:

    - Telemediengesetz (TMG), z.B. Impressumspflicht
    - Urheberrechtliche und wettbewerbsrechtliche Regelungen
    - Dienstrechtliche Regelungen

[16] Ein Verbot der privaten Nutzung ist in bestimmten Verwaltungsbereichen möglich, z.B. wenn hierdurch bei der Polizei Fahndungserfolge oder Kollegen gefährdet werden. Die Verbote sollten dort dann speziell geregelt werden.

- Personalvertretungsgesetz

11. **Kontrolle behalten:** Wenn im Rahmen der Optimierung Social Media in die dienstliche Aufgabenerledigung mit einbezogen wird, sind Rahmenbedingungen zu schaffen, um die Kontrolle über die Aufgabenerledigung zu behalten. Z.B. ist auf Folgendes zu achten:

    - Manipulationen müssen verhindert werden. Z.B. muss sichergestellt sein, dass auf Präsentationen der Behörde keine Unbefugten schreibend zugreifen können.
    - Der Social-Media-Dienst muss dauerhaft zur Verfügung stehen.
    - Es muss weiterhin eine vollständige, transparente Aktenführung gewährleistet sein[17].
    - Die für geschlossene Benutzergruppen bereitgestellten Daten dürfen nur Befugten zugänglich sein.
    - Die Unterstützung durch den Social-Media-Dienst sollte durch eine andere Unterstützung ersetzbar sein.

    Insbesondere wenn sensible Daten (z.B. Personaldaten, Unterlagen in Vergabeverfahren) durch einen Diensteanbieter im Internet verarbeitet werden sollen, muss die Behörde als Auftraggeber durch klare, ggf. individuelle vertragliche Regelungen mit dem Anbieter für eine rechtlich einwandfreie Datenverarbeitung sorgen. Wenn Social-Media-Dienste solche Regelungen nicht akzeptieren, muss die Verarbeitung unterbleiben.

12. **Bedienstete schützen:** Bei Behördenauftritten ist auch der Schutz der Privatsphäre von Bediensteten zu berücksichtigen. Diese dürfen nicht dazu gezwungen werden, eigene oder andere personenbezogene Daten in sozialen Medien preiszugeben. Soweit Kennungen bereitgestellt werden müssen, sind Funktionskennungen zu verwenden. Die Pflichten zur Beteiligung des Personalrats sind zu beachten.

13. **Geschlossene Benutzergruppen:** Wenn Social Media nur von Bediensteten der Verwaltung genutzt werden sollen, sollten interne Angebote verwendet werden. Intranet-Präsentationen, Community-Plattformen, Foren oder Wikis können z.B. mithilfe des Content-Management-Systems des Landesintranets betrieben werden. Kollaborations- und eAkte-Systeme stellt der LSKN auf Anforderung gegen Entgelt bereit.

14. **Geschäftsbedingungen beachten:** Vor der Einrichtung eines Behördenauftritts sind die Geschäftsbedingungen des Social-Media-Anbieters genau zu prüfen.

15. **Nutzerinnen und Nutzer über Risiken informieren:** Nutzerinnen und Nutzer müssen über Risiken informiert werden, die sie bei Nutzung eines Behördenauftritts eingehen. Dies gilt insbesondere, wenn die Einwilligung der Betroffenen eingeholt werden muss („informierte Einwilligung“). Die wichtigsten Hinweise betreffen folgende Punkte:

    - Kontaktdaten der für die Datenverarbeitung verantwortlichen Stelle.
    - Zweck und Umfang der Datenverarbeitung und Verbleib der personenbezogenen Daten.
    - Eingaben, die nicht veröffentlicht werden, möglichst per SSL-Verschlüsselung (https) versenden, um unbefugtes Mitlesen zu verhindern.

    Wenn die Nutzung mit erheblichen Risiken verbunden ist, muss es alternative Informations- bzw. Beteiligungsangebote geben. Wenn Nutzerinnen und Nutzer sensible perso-

[17]. Aktenrelevante Daten dürfen daher nicht ausschließlich in Social-Media-Angeboten gespeichert werden, sondern sind nach der Nds. Aktenordnung aufzubewahren.

nenbezogene oder sicherheitsrelevante Daten übermitteln und hierauf eine Antwort erwarten, sollten diese so beantwortet werden, dass diese gegen Zugriff geschützt übermittelt werden. Ist dies nicht möglich, ist auf eine Übermittlung zu verzichten.

16. **Behördenpräsentation erfordert Freigabe:** Ist vorgesehen, die Behörde oder Teile von ihr in den Social Media zu präsentieren, so ist vorher die Stelle für Öffentlichkeitsarbeit zu beteiligen[18]. Diese Stelle hat die Freigabe der Präsentation zu erteilen. Abhängig von der Art der Präsentation sollte diese Freigabe einmalig mit dauerhafter Gültigkeit oder für jede Änderung eingeholt werden. Presseinformationsähnliche Veröffentlichungen sollten immer von der für Öffentlichkeitsarbeit zuständigen Stelle freigegeben werden.

17. **Social-Media-Netiquette beachten**: Beim Umgang mit Social Media sollten Behörden auf den passenden Umgangsstil achten. Z.B. sollten folgende Punkte beachtet werden:

    - Allgemeinverständliche, kurze Texte verwenden!
    - Auf dienstlichen Charakter hinweisen!
    - Sachlich und korrekt, nicht verletzend formulieren!
    - Formulierungen adressatengerecht, aber in amtlicher deutscher Rechtschreibung!
    - Nicht abgestimmte Auffassungen als solche kennzeichnen!
    - Quellen, Urheber angeben!

18. **Missbrauch von Behördenidentitäten**: Verwenden Nutzerinnen und Nutzer Behördenidentitäten missbräuchlich (z.B. wenn fremde Personen sich als Sprecher einer Behörde ausgeben), sind verschiedene Gegenmaßnahmen denkbar. Sie richten sich nach dem Schadensausmaß des Missbrauchs und den Möglichkeiten, den Missbrauch einzuschränken. Ggf. sind der entsprechende Nutzer oder die Nutzerin, der Dienstanbieter oder die zuständige Polizeibehörde auf den Missbrauch hinzuweisen. Sichern Sie hierzu die Kommunikationsdaten, um den Missbrauch deutlich zu machen.

19. **Umgang mit Social Plug-ins**: Über soziale Erweiterungsmodule (englisch „Social Plugins“) können Website-Betreiber einfach kleine Anwendungen mit minimalem Programmieraufwand im eigenen Portal integrieren. Die beliebtesten Plug-ins sind der *Like Button*, die *Like Box* und die *Facebook Comment Box.* Der IT-Planungsrat[19] des Bundes und der Länder empfiehlt, von der direkten Einbindung von Social Plug-ins ohne Einwilligungsmöglichkeit abzusehen. Wenn Behördenseiten dennoch Links zu Social Media enthalten sollen, müssen daher die Nutzer vor einer Übertragung von Daten ausreichend informiert werden. Dies kann beispielsweise mit dem folgenden Textbaustein erfolgen:

    - Durch Anklicken dieses Links werden bestimmte Daten, die Ihr Internet-Browser speichert, für xyz verfügbar. Hierzu gehören die IP-Adresse, die aktuelle URL sowie Cookies, die xyz in früheren Sessions auf Ihrem Rechner abgespeichert wurden. Sie müssen damit rechnen, dass xyz diese Daten abruft, Ihrem Account zuordnet und auswertet. Verwenden Sie diesen Link nur, wenn Sie mit dieser Datenverarbeitung

[18] Die Behörde kann eine hiervon abweichende Regelung treffen.
[19] Beschluss des IT-Planungsrat vom 8.03.2012, TOP 17

einverstanden sind.

Im Internet werden Lösungen[20] beschrieben, wie an sich unzureichende social Plug-ins mithilfe von vorgeschalteten „Aktivierungs-Buttons“ so eingesetzt werden können, dass die datenschutzrechtlichen Anforderungen erfüllt werden.

[20] Z. B. http://www.heise.de/ct/artikel/2-Klicks-fuer-mehr-Datenschutz-1333879.html