Unsere Freiheiten:
Daten nützen - Daten schützen

Wesentliche Anforderungen
an die behördliche Nutzung „Sozialer Netzwerke“

Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Der Landesbeauftragte für den Datenschutz
und die Informationsfreiheit Baden-Württemberg

Dr. Stefan Brink

Königstraße 10a
70173 Stuttgart

Telefon: (07 11) 61 55 41-0
Telefax: (07 11) 61 55 41-15

E-Mail: poststelle@lfdi.bwl.de
Homepage: https://www.baden-wuerttemberg.datenschutz.de/

Schutzbedürftige Daten sollten nicht unverschlüsselt per E-Mail oder via Telefax übertragen werden.
PGP-Fingerprint: E4FA 428C B315 2248 83BB F6FB 0FC3 48A6 4A32 5962

Stand: Februar 2020

Wesentliche Anforderungen
an die behördliche Nutzung „Sozialer Netzwerke“

„Soziale Netzwerke“ sind Internet-Plattformen, die der Kommunikation, Interaktion und Präsentation ihrer Mitglieder und somit dem Austausch von Informationen dienen. Sie sind inzwischen zu einem wesentlichen Bestandteil des privaten und beruflichen Lebens geworden. Beispiele für solche Plattformen sind u.a. Facebook, Instagram und Twitter.

Solche Plattformen basieren häufig auf profilbasierten technischen Lösungen, das heißt die Erfassung, systematische Speicherung und Verwertung personenbezogener Daten ihrer Mitglieder und ggf. auch von Bürgerinnen und Bürgern, die nicht Mitglieder sind, ist wesentlicher Teil ihres Geschäftsmodells.

Aufgrund der Vielzahl und der Sensibilität der dort verarbeiteten personenbezogenen Daten muss der Schutz betroffener Personen gerade im Bereich „Sozialer Netzwerke“ dadurch gewährleistet werden, dass die datenschutzrechtlichen Vorschriften konsequent eingehalten werden. Diese Schutzvorschriften verpflichten nicht nur den Plattformbetreiber selbst, sondern auch deren behördliche Mitglieder.

Dabei sind insbesondere folgende Anforderungen einzuhalten:

1. Behördliche Mitglieder müssen eine **datenschutzrechtliche Rechtsgrundlage** vorweisen können.

2. Die datenschutzrechtlichen **Transparenzgebote** müssen eingehalten werden.

3. Soweit behördliche Mitglieder mit dem Plattformbetreiber zusammen **gemeinsam verantwortlich** für Datenverarbeitungen sind, muss dazu eine **vertragliche Vereinbarung** getroffen werden.

4. Behördliche Mitglieder müssen **alternative Informations- und Kommunikationswege** anbieten, damit Bürgerinnen und Bürger nicht in „Soziale Netzwerke“ hineingezwungen werden.

5. Die **technischen und organisatorischen Sicherungsmaßnahmen** müssen dem Stand der Technik genügen und der **Selbstschutz der Bürgerinnen und Bürger** muss respektiert werden.

Sind diese Anforderungen aktuell bei der Nutzung „Sozialer Netzwerke“ durch Behörden nicht erfüllt, so muss jetzt umgehend nachgebessert werden. Dies setzt die Kooperation des jeweiligen Plattformbetreibers voraus.

Kooperiert der Plattformbetreiber mit der Behörde nicht und gelingt es dieser nicht, die einschlägigen Vorgaben zu erfüllen, so ist die Plattform zu verlassen.

Dies bedeutet im Einzelnen:

- Jede Phase der Verarbeitung personenbezogener Daten im Rahmen der Nutzung „Sozialer Netzwerke“ durch Behörden benötigt jeweils eine eigene **Rechtsgrundlage** (vgl. zur Datenschutz-Grundverordnung (DS-GVO) Artikel 6).

  Öffentliche Stellen nutzen „Soziale Netzwerke“ in der Regel für ihre **Öffentlichkeitsarbeit**. Sie handeln dabei **in Erfüllung einer öffentlichen Aufgabe**, die Verarbeitung personenbezogener Daten für ihre Öffentlichkeitsarbeit ist ihnen grundsätzlich durch Artikel 6 Absatz 1 Satz 1 Buchstabe e), Absatz 2 und 3 DS-GVO in Verbindung mit § 4 Landesdatenschutzgesetz Baden-Württemberg (LDSG BW) erlaubt. Ob § 4 LDSG die Anforderungen des Art. 6 Abs. 2 und 3 DS-GVO erfüllt, ist allerdings umstritten.

  Werden die Daten der Bürgerinnen und Bürger über die Öffentlichkeitsarbeit hinaus etwa zur Analyse des Nutzerverhaltens ausgewertet, so ist dies für die Öffentlichkeitsarbeit der Behörde nicht mehr erforderlich und nicht mehr von dieser Rechtsgrundlage gedeckt. Infrage käme dafür nur noch eine **Einwilligung** nach Artikel 6 Absatz 1 Satz 1 Buchstabe a) DS-GVO. Eine freiwillige, vorherige, aktive, konkrete und separat erklärte sowie jederzeit zumutbar (mit Wirkung für die Zukunft) widerrufliche Einwilligung nach Artikel 6 Absatz 1 Satz 1 Buchstabe a) DS-GVO ist notwendig, wenn
  - über den Mitglieds-Account der Behörde personenbezogene Daten (z.B. über das Nutzerverhalten) der Bürgerinnen und Bürger gesammelt oder weitergegeben werden (z.B. mittels permanenter Cookies oder anderer Tracking-Mechanismen),
  - auf der eigenen Website oder App der Behörde Elemente wie Plug-Ins oder eingebettete Nachrichten von „Sozialen Netzwerken“ oder anderen Dritten ohne datenschutzfreundliche Implementierung (sichere Zwei-Klick-Lösung) eingebettet werden und diese die Verarbeitung von Daten über die Nutzung durch Bürgerinnen und Bürger ermöglichen,
  - externe einwilligungsbedürftige Analyse-Tools wie etwa Google Analytics eingebunden werden oder
  - persönliche Informationen von Bürgerinnen und Bürgern beispielsweise aus Adressbüchern hochgeladen werden.

  Auf ein berechtigtes Interesse im Sinne des Artikel 6 Absatz 1 Satz 1 Buchstabe f) DS-GVO können sich Behörden nach Artikel 6 Absatz 1 Satz 2 DS-GVO nie berufen.

  In Fällen, in denen nicht eine reine Öffentlichkeitsarbeit durchgeführt wird, sondern beispielsweise mittels der Nutzung „Sozialer Netzwerke“ die öffentliche Sicherheit gewährleistet wird (Warnung vor Umweltkatastrophen oder terroristischen Anschlägen), kann der behördliche Auftritt in „Sozialen Netzwerken“ auch gestützt auf Artikel 6 Absatz 1 Satz 1 Buchstabe e), Absatz 2 und 3 DS-GVO in Verbindung mit einer speziellen fachgesetzlichen Rechtsgrundlage erfolgen.

  Aufgrund dieser insgesamt nur schwer nachvollziehbaren und teilweise unklaren Rechtslage ist der Gesetzgeber dazu aufgerufen zu prüfen, ob durch ein **Gesetz zur Öffentlichkeitsarbeit von Behörden** künftig mehr Rechtssicherheit geschaffen werden kann.

- Jegliche Verarbeitung personenbezogener Daten muss **transparent** gemacht werden (vgl. Artikel 13 und 14 DS-GVO). Eine beispielhafte Aufzählung von Datenverarbeitungen genügt dafür nicht. Neben der Angabe von Rechtsgrundlage, Zweck und verarbeiteten Datenkategorien ist auch über eine etwaige Weitergabe personenbezogener Daten der Bürgerinnen und Bürger an Dritte zwingend zu informieren. Bei der Verwendung von Cookies oder ähnlichen Techniken zur Wiedererkennung von nutzenden Bürgerinnen und Bürgern müssen Zwecke und die Dauer solcher Tracking-Maßnahmen angegeben werden.

- Wer einen solchen Dienst als Behörde nutzt, ist zunächst dafür verantwortlich, was er selbst dort tut. Soweit die behördlichen Mitglieder mit dem Plattformbetreiber zusammen **gemeinsam verantwortlich** und haftbar sind (vgl. dazu EuGH C-210/16)[1], erstreckt sich ihre Verantwortlichkeit auch auf Datenverarbeitungen durch den Plattformbetreiber und auf die gemeinsame Erfüllung von Betroffenenrechten wie Auskunfts-, Lösch- oder Schadensersatzpflichten. Das Argument, man habe auf den Betreiber der gewählten Plattform nur beschränkt Einfluss (Blackbox-Argument), ist bei einer gemeinsamen Verantwortlichkeit kein gültiges Argument.

  Liegt eine gemeinsame Verantwortlichkeit vor, so müssen Account-Inhaber und Plattform-Betreiber in einer **Vereinbarung** transparent festlegen, wer von ihnen welche Verpflichtung gemäß DS-GVO erfüllt. Eine solche Aufteilung der Pflichten ist aber nur möglich, wenn - anders als etwa in dem aktuell von Facebook bereitgestellten Addendum und den Datenschutzhinweisen – tatsächlich alle Verarbeitungen personenbezogener Daten vollständig offen gelegt werden. Die wesentlichen Inhalte dieser Vereinbarung nach Art. 26 DS-GVO müssen zudem den Bürgerinnen und Bürgern, die das Informationsangebot nutzen, zur Verfügung gestellt werden.[2]

- **Alternative Informations- und Kommunikationswege** müssen vom behördlichen Mitglied angeboten werden. Einwilligungen können bei der behördlichen Nutzung von „Sozialen Netzwerken“ nur dann als freiwillig betrachtet werden, wenn es den Bürgerinnen und Bürgern auch möglich ist, sich der Verarbeitung der eigenen personenbezogenen Daten durch einen Plattformbetreiber über die Nutzung alternativer Angebote wie etwa einer Behörden-Webseite zu entziehen. Die Landesregierung hat sich bereits im Bereich der Kurznachrichtendienste dazu entschlossen, einen solchen alternativen Kommunikationskanal auf Mastodon – einem dezentralen Kurznachrichtendienst – anzubieten.[3] Näheres findet sich hierzu in der „Richtlinie des LfDI zur Nutzung von Sozialen Netzwerken durch öffentliche Stellen“[4].

---

1 Siehe die Entscheidung des Europäischen Gerichtshofs vom 5. Juni 2018 (C-210/16), in der eine gemeinsame Verantwortlichkeit (vgl. Artikel 26 DS-GVO) des „Sozialen Netzwerks“ Facebook und dessen Mitgliedern festgestellt wurde.

2 Muster für eine solche Vereinbarung und die Informationen, die weitergegeben werden müssen, erhalten Sie unter: https://www.baden-wuerttemberg.datenschutz.de/datenschutzthemen/

3 https://mastodon.social/@RegierungBW

4 Siehe dazu die Richtlinie des LfDI zur Nutzung von Sozialen Netzwerken durch öffentliche Stellen im Anhang

- Die **technischen und organisatorischen Sicherungsmaßnahmen von Plattform und Behörden-Account** müssen dem Stand der Technik entsprechen und den **Selbstschutz der Bürgerinnen und Bürger** respektieren. Von Bürgerinnen und Bürgern im Browser gewählte Schutzmaßnahmen (z.B. Einstellungen zu Cookies, Do-Not-Track, Deaktivierung von Standortdaten, Blockierung von bestimmten Domains) dürfen weder vom Plattformbetreiber noch vom behördlichen Mitglied ausgeschaltet oder umgangen werden.

Richtlinie des LfDI zur Nutzung von Sozialen Netzwerken durch öffentliche Stellen (2017, überarbeitet 2020)

I. Worum geht es?

1. Soziale Netzwerke – anscheinend unverzichtbar

Soziale Netzwerke wie Facebook, Twitter oder Instagram sind zu einem wesentlichen Bestandteil des beruflichen und privaten Informations- und Kommunikationsverhaltens vieler Bürgerinnen und Bürger geworden. Auch öffentliche Stellen nutzen vermehrt Soziale Netzwerke oder planen dies für die Zukunft: Sicherheitsbehörden möchten via Twitter aktuelle Kurzhinweise an Teilnehmer von Versammlungen geben, Kommunen über Facebook auf ihr touristisches Angebot hinweisen und Anfragen dazu beantworten, und nicht wenige Behörden rekrutieren ihren Nachwuchs über Soziale Netzwerke.

Die vorliegende Richtlinie zielt in erster Linie auf die Nutzung Sozialer Netzwerke zu Zwecken der **Öffentlichkeitsarbeit** und der **Bereitstellung allgemeiner Informationen der Verwaltung** (Aufgaben, Leistungen, Öffnungszeiten, Kontaktdaten, Ansprechpartner, Hinweise auf Veranstaltungen, Diskussionsmoderation etc.), nicht aber zur Bereitstellung bzw. zum Bezug konkreter Verwaltungsleistungen. Diese Aspekte regeln die bestehenden oder noch zu schaffenden E-Government-Gesetze.

2. Grenzen der Nutzung durch öffentliche Stellen

Während die Nutzung Sozialer Netzwerke durch die Bürger in deren Belieben gestellt ist, unterliegen **öffentliche Stellen** insoweit **vielfältigen gesetzlichen Bindungen** und haben zudem eine **rechtsstaatlich begründete Vorbildfunktion**. Hierauf haben Datenschützer immer wieder warnend hingewiesen, wurden damit aber (zu) selten gehört. Mit der jetzt vorgelegten Orientierungshilfe soll dem Nutzungsinteresse der öffentlichen Stellen ebenso Rechnung getragen werden wie den für öffentliche Stellen bestehenden datenschutzrechtlichen Grenzen.

3. Um Messenger geht's hier nicht

Der Fokus dieser Richtlinie liegt also auf Sozialen Netzwerken, die sich als Plattformen an die Öffentlichkeit richten. Die Nutzung sog. Instant-Messaging-Dienste wie etwa WhatsApp, Snapchat und des Facebook-Messengers unterliegt strengeren Voraussetzungen – gerade in den Fällen, in denen zwischen Staat und Nutzern eine besondere Schutz- und Obhutsbeziehung besteht, wie etwa im Bereich von Kindergärten oder Schulen – und ist daher nicht Gegenstand dieser Richtlinie.

4. Juristisch betrachtet …

Bei Sozialen Netzwerken handelt es sich rechtlich um **Telemedien** nach § 1 Abs. 1 des Telemediengesetzes (TMG). Aufgrund der entstandenen zeitlichen Verzögerung im Gesetzgebungsverfahren zum Erlass der ePrivacy-Verordnung und der teilweise nicht hinreichenden Umsetzung der alten ePrivacy-Richtlinie ist die DS-GVO jedoch im Bereich von Kapitel 4 des TMG vorrangig anzuwenden und verdrängt dessen Vorschriften (siehe dazu die Positionsbestimmung der DSK „Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018“).

Bei Sozialen Netzwerken handelt es sich vielfach um **gestufte Anbieterverhältnisse**, bei denen der jeweilige Informations- oder Kommunikationsdienst auf einer Plattform angeboten wird. Dem Nutzer stehen also der jeweilige **Inhalteanbieter**, der die Plattform nutzt, um sich zu präsentieren, dort Inhalte zu posten oder zu kommentieren (darunter fallen nunmehr auch öffentliche Stellen), und der jeweilige **Plattformbetreiber** gegenüber. Dies macht Soziale Netzwerke aus Nutzerperspektive schwer durchschaubar und aus rechtlicher Sicht häufig problematisch, gerade im Hinblick auf datenschutzrechtliche Verantwortlichkeiten. Insbesondere im Fall außereuropäischer Plattformbetreiber/-anbieter sind **grundlegende Rechtsfragen letztlich nicht geklärt**.

Vorgaben etwa des Wettbewerbsrechts, des Vergaberechts oder besondere öffentlich-rechtliche Bindungen von Behörden sind nicht Gegenstand dieser Richtlinie. Dass es hier weitere Regeln für öffentliche Stellen zu beachten gilt, etwa bei der vertraglichen Anbindung an Monopolisten im Bereich der Internet-Kommunikation, liegt auf der Hand.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit (LfDI) sieht jedenfalls eine **datenschutzrechtliche Mitverantwortung öffentlicher Stellen**, die Soziale Netzwerke im Rahmen ihrer Aufgabenerfüllung einsetzen, da erst durch deren Angebote in Sozialen Netzwerken entsprechende Nutzungsdaten entstehen, die vom jeweiligen Plattformbetreiber verarbeitet werden können. Aus dieser Verantwortung ergeben sich **Rechtspflichten der öffentlichen Stellen** (dazu sogleich unter II.).

5. Was genau bedeutet das?

Auch bei der Nutzung Sozialer Netzwerke durch öffentliche Stellen gilt also: **keine Chance ohne Grenzen**. Staatliche und kommunale Stellen unterliegen einer verfassungsrechtlichen Bindung an Recht und Gesetz (Rechtsstaatsprinzip) und stehen aufgrund ihrer gesellschaftlichen Vorbildfunktion in einer besonderen Verantwortung – auch bei der Nutzung Sozialer Netzwerke. Angesichts offensichtlicher **datenschutzrechtlicher Defizite** bei einer Reihe Sozialer Netzwerke sollen die öffentliche Stellen ihre dortigen Angebote zukünftig auf **Datensparsamkeit** bei der Verarbeitung von Nutzungsdaten und auf eine **aktive Information der Nutzerinnen und Nutzer** über die angesprochenen Gefahren für deren persönliche Daten ausrichten. Fehlende Widerspruchsmöglichkeiten bei Sozialen Netzwerken selbst sind durch Maßnahmen der öffentlichen Stellen wie Information und **Aufklärung**, einen Hinweis auf die eigenverantwortliche Nutzung und auf das **Angebot alternativer Kommunikationskanäle** zu kompensieren, um die Nutzerinnen und Nutzer in die Lage zu versetzen, über ihre Daten tatsächlich selbst zu bestimmen.

II. Vorgaben und Voraussetzungen

Aus Sicht des LfDI haben öffentliche Stellen bei einer Nutzung Sozialer Netzwerke daher folgende **vier Punkte** zu berücksichtigen: Es muss 1. ein **Nutzungskonzept** festgelegt werden, 2. sind die **Pflichten** nach dem TMG einzuhalten, 3. muss die öffentliche Stelle ihren Auftritt kontinuierlich betreuen und 4. sind **alternative Informations- und Kommunikationswege** anzubieten.

1. Klares Konzept

a) Vor der Nutzung eines Sozialen Netzwerks muss die öffentliche Stelle ein Konzept erstellen, welches **Zweck, Art und Umfang der vorgesehenen Nutzung** Sozialer Netzwerke durch die öffentliche Stelle beschreibt, die Gründe der Entscheidung für das gewählte Soziale Netzwerk darstellt sowie Verantwortlichkeiten für die redaktionelle/technische Betreuung und die Wahrnehmung der Rechte der Betroffenen nach Artt. 15 ff. der Europäischen Datenschutz-Grundverordnung (DS-GVO) festlegt. Dabei muss erkennbar sein, welche Vorteile sich die jeweilige Stelle für ihre Aufgabenerfüllung durch die Nutzung erhofft bzw. welche Nachteile durch einen Verzicht entstehen würden.
Dieses Konzept bildet die Grundlage für zukünftige Prüfungen des LfDI.

b) Die jeweiligen Nutzungszwecke führen notwendig zu **Differenzierungen**, die sich im Konzept wiederfinden müssen: Im Rahmen der Öffentlichkeitsarbeit eines Ministeriums können andere Schwerpunkte zum Tragen kommen als bei der Öffentlichkeitsarbeit einer Verbandsgemeinde oder der Öffentlichkeitsarbeit zum Zweck der Nachwuchsgewinnung. Auch können sich Unterschiede im Hinblick auf den Umfang der intendierten Nutzung ergeben, je nachdem, ob nur eine **bloße Information** oder auch eine **Kommunikation** mit den Bürgern vorgesehen ist. Insbesondere bei letzterer ist auf einen sorgfältigen Umgang gerade auch mit sensiblen Daten zu achten.

c) Im Rahmen des Konzepts ist auch eine **Abschätzung der Konsequenzen der vorgesehenen Verarbeitungsvorgänge** für den Schutz personenbezogener Daten, vorzunehmen. Eine Meldepflicht gegenüber dem LfDI besteht insoweit in der Regel nicht – aber wir beraten natürlich gerne.

d) Das Konzept sollte anhand der gemachten Erfahrungen regelmäßig, mindestens jährlich auf Erforderlichkeit und Ausmaß der Nutzung des Sozialen Netzwerks **evaluiert** werden.

e) Das entwickelte Konzept und dessen Evaluation sind allgemein zugänglich zu machen, etwa nach Vorbild des § 11 Landesinformationsfreiheitsgesetz (LIFG) im Internet zu **veröffentlichen**.

2. Gestaltung des eigenen Netzwerk-Angebots: TMG-Pflichten beachten!

a) Das eigene Angebot muss Angaben gemäß § 5 TMG enthalten, welche **die öffentliche Stelle als Anbieter erkennen lassen**. Diese Angaben müssen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sein. Dem wird entsprochen, wenn die Angaben als „Impressum“ oder „Kontakt“ bezeichnet werden, im allgemeinen Navigationsmenü als eigener Punkt untergebracht und mit maximal zwei Schritten erreichbar sind.

b) Das Angebot muss über eine **eigene Datenschutzerklärung** verfügen, die als solche zu bezeichnen ist und wie das Impressum im Navigationsmenü als eigener Punkt untergebracht sein sollte, im Gegensatz zu diesem aber von jeder Seite des Angebots, also in einem Schritt, erreichbar sein muss. Zudem muss sie das eingangs beschriebene gestufte Anbieterverhältnis widerspiegeln:

   a. So muss die Datenschutzerklärung die Nutzerinnen und Nutzer einerseits über eine Verarbeitung von **Nutzungsdaten durch den Plattformbetreiber** und eine etwaige Übermittlung der Daten außerhalb der Europäischen Union unterrichten; dabei ist auch auf die Datenschutzerklärung des Plattformbetreibers zu verlinken und auf die bei Sozialen Netzwerken bestehenden datenschutzrechtlichen Probleme sowie auf bestehende Möglichkeiten, die Verarbeitung von Nutzungsdaten einzuschränken, hinzuweisen (Datenschutz-/Privatsphäreneinstellungen des jeweiligen Sozialen Netzwerks). Wenn bei dem genutzten Sozialen Netzwerk keine dauerhaft verfügbare Datenschutzerklärung bereitgestellt werden kann, ist den Nutzerinnen und Nutzern ein **regelmäßiger Hinweis** auf diese zu geben (abhängig von der Häufigkeit neuer Inhalte jedenfalls monatlich), verbunden mit einem entsprechenden Link auf den Text der eigenen Datenschutzerklärung.

      Außerdem soll auf die Eigenverantwortung der registrierten Nutzerinnen und Nutzer für die Inanspruchnahme der Social-Media-Dienste Bezug genommen und ein **Hinweis auf die bestehenden alternativen Informations- und Kommunikationswege** gegeben werden, also z.B. die E-Mail-Adresse der Behörde oder die Behörden-Webseite.

      Soweit Mechanismen zum Einsatz kommen, mit denen durch den Plattformbetreiber eine Nutzung außerhalb desjeweiligen Sozialen Netzwerks erfasst werden kann (z.B. Cookies, Social Plug-Ins), sind die Nutzerinnen und Nutzer auch auf diese hinzuweisen, z.B. mittels eines entsprechenden Cookie-Banners oder Hinweis-Textes. Bei der Verwendung von Social Plug-Ins ist die 2-Klick- bzw. die Shariff-Lösung zu verwenden. Sind Plug-Ins auf diese Weise implementiert, werden nicht schon mit dem Aufruf der Internetseite personenbezogene Daten übermittelt, sondern erst nach Aktivierung des Plug-Ins per Mausklick.

      Der öffentlichen Stelle obliegt hier eine **eigene Informations-und Prüfpflicht**.

   b. Andererseits muss die Datenschutzerklärung eine **Unterrichtung nach § 13 TMG** enthalten (Art, Umfang, Zweck der Verarbeitung), soweit über das Soziale Netzwerk personenbezogene Daten durch die öffentliche Stelle selbst erhoben und verarbeitet werden. In diesem Zusammenhang sind die Vorgaben nach Artt. 44 ff. DSGVO zu beachten (**Datenübermittlung ins Ausland**). Die öffentliche Stelle trägt dabei eine Mitverantwortung für die Erhebung von Daten durch das Soziale Netzwerk über die Personen, die die Seite des Netzwerks besuchen; werden durch das Soziale Netzwerk

z.B. personenbezogene Daten mittels Cookies erhoben und daraus Besucherstatistiken für die öffentliche Stelle erstellt, so trägt die öffentliche Stelle für diese Erhebung eine Mitverantwortung und muss Besucher ihrer Netzwerk-Seite auf diese Erhebung hinweisen.

3. Kontinuierliche Betreuung des eigenen Angebots

Gemäß § 7 Abs. 1 TMG sind Diensteanbieter grundsätzlich nur für eigene Informationen, die sie zur Nutzung bereithalten, verantwortlich, nicht jedoch für fremde Inhalte und Datenverarbeitungen. Dies hat zur Folge, dass ein Diensteanbieter nicht verpflichtet ist, die von den Nutzern in das Netz gestellten Beiträge vor der Veröffentlichung auf eventuelle Rechtsverletzungen zu überprüfen. Besteht jedoch seitens der Nutzer die Möglichkeit, im Rahmen des Angebots der öffentlichen Stelle interaktiv teilzunehmen (z.B. durch Kommentare), und erlangt die öffentliche Stelle Kenntnis von einer rechtswidrigen Handlung oder Information, so haftet sie nach § 10 TMG, wenn sie nicht unverzüglich tätig wird und die Informationen entfernt. Die öffentliche Stelle muss ihr Angebot daher – ihrem Konzept entsprechend – von einer **entsprechend geschulten Person redaktionell betreuen** lassen.

Übernahme von Verantwortung bedeutet auch, in dem genutzten Sozialen Netzwerk regelmäßig (mindestens einmal im Quartal) **Aktionen zur Sensibilisierung der Nutzerinnen und Nutzer** hinsichtlich der Risiken für ihr Recht auf informationelle Selbstbestimmung durchzuführen. Dies kann beispielsweise durch Hinweise auf aktuelle Datenschutzthemen, auf Beiträge zum Datenschutz oder durch Hinweise auf entsprechende Informationsangebote erfolgen.

4. Alternativen anbieten

a) Grundsätzlich darf der Zugang zu Informationen der öffentlichen Stelle nicht von einer vorherigen Registrierung bei einem Sozialen Netzwerk abhängig sein. Außer über das Soziale Netzwerk müssen die bereitgestellten Informationen daher **immer auch auf einem alternativen Weg** verfügbar sein (z.B. Webseite der Verwaltung). In keinem Fall darf eine Situation entstehen, in der Nutzerinnen und Nutzer veranlasst werden, ein Soziales Netzwerk nur deswegen zu nutzen, weil sie nur dort bestimmte staatliche oder kommunale Informationen bekommen.

b) Das Angebot von Alternativen gilt besonders im Hinblick auf die **Nutzung interaktiver Funktionen** (z.B. Kommentieren, Teilen, Bewerten). Diese geht über ein reines Informationsangebot hinaus und steht weitgehend in der Verantwortung der Nutzerinnen und Nutzer. Soweit die Funktionen darauf ausgerichtet sind, in einen intensivierten Dialog mit der öffentlichen Stelle zu treten, ist immer auch eine **alternative Kommunikationsmöglichkeit** außerhalb des Sozialen Netzwerks **anzubieten** (z.B. E-Mail/Telefon). Die öffentliche Stelle kann nach Maßgabe der Erforderlichkeit interaktive Funktionen nutzen, etwa auf aktuelle Geschehnisse und Gefahrenlagen hinweisen, auf Kommentare und Fragen antworten und Kommunikation moderieren, wenn Verarbeitung und Übermittlung personenbezogener Daten so weit wie möglich vermieden werden und auf die Nutzung alternativer Wege nachdrücklich hingewirkt wird.

III. Ausblick

Damit steht aus Sicht des LfDI ein Handlungsrahmen zur Verfügung, mit dem Erwartungen von Nutzerinnen und Nutzern an eine Beteiligung öffentlicher Stellen an Sozialen Netzwerken entsprochen werden kann und der trotz weiterhin offener Punkte anerkannte Datenschutzstandards wirksam werden lässt.

Europäische Rechtsvorschriften zum Datenschutz, die seit Mai 2018 wirksam sind, erlegen den Anbietern von Sozialen Netzwerken weit reichende Pflichten, insbesondere auch hinsichtlich der Transparenz und der Information des Einzelnen auf. Dies hat auch bei öffentlichen Stellen, die Soziale Netzwerke nutzen, bereits zu Anpassungen geführt. Die dynamische Entwicklung in diesem Bereich wird für weiteren Anpassungsbedarf sorgen. Der LfDI beobachtet diese Entwicklung und wird auch zukünftig Beratung und Unterstützung anbieten.