Ständige Arbeitsgruppe Datenschutz, Melderecht und IT-Recht sowie
Ständige Arbeitsgruppe Urheberrecht
der Rechtskommission des VDD

(Dezember 2013)

Nutzung sozialer Netzwerke (social networking) in Einrichtungen der Katholischen Kirche

Aktuelle Anforderungen an den kirchlichen Datenschutz, das Urheberrecht u.a. am Beispiel „Facebook“

Inhaltsverzeichnis:

Einleitung:

„Rund 22 Millionen Nutzer hat allein das soziale Netzwerk „Facebook" derzeit in Deutschland. Ein großer Teil davon sind Arbeitnehmer, die „Facebook" für die Pflege privater wie beruflicher Kontakte nutzen: Soziale Netzwerke vereinfachen die Kommunikation, sie ermöglichen es, Informationen schnell mit einer großen Anzahl von Freunden, Bekannten, Kollegen und Geschäftspartnern zu teilen."[1]

Auch in kirchlichen Einrichtungen haben soziale Netzwerke, im Besonderen „Facebook", mittlerweile einen hohen Verbreitungsgrad, sei es als offizielle „Fanpage" der Abteilungen und Dienststellen für Öffentlichkeitsarbeit auf Bistumsebene (neben der jeweiligen Bistumshomepage), als persönliche Facebook-Profile von Priestern und kirchlichen Mitarbeitern/-innen oder als Gruppen-Profile für Veranstaltungen pfarrlicher Jugendgruppen. Die Nutzung sozialer Netzwerke durch Einrichtungen der Katholischen Kirche wird wegen ihres hohen Verbreitungsgrades gerade bei der jüngeren Generation als zeitgemäße Möglichkeit zum Transport und zur positiven Vermittlung pastoraler Anliegen, ja *„als Ort der Neuevangelisierung gesehen".*[2] Dies erscheint legitim, vor allem da nach der jüngsten Bitkom-Studie (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.) die meisten Internet-User sich *rund 1 Stunde täglich in sozialen Netzwerken aufhalten.*[3]

Da nach der gleichen Studie *„Facebook" bei der Gruppe der 14 – 29 jährigen einen Verbreitungsgrad von 72 % hat und jeder dieser Nutzer im Durchschnitt über 133 „Freunde" verfügt*[4], erscheinen die Möglichkeiten zum positiven Vermitteln pastoraler Anliegen über soziale Netzwerke geradezu evident.

Aus datenschutz- und urheberrechtlicher Sicht sowie aus Gründen der „Unternehmenssicherheit" ergeben sich allerdings eine Fülle von Anforderungen und Fragestellungen für die kirchlichen Nutzer sozialer Netzwerke, die nachstehend am Beispiel „Facebook" lediglich skizzenhaft dargestellt werden.

---

[1] Bayerisches Landesamt für Verfassungsschutz: „Soziale Netzwerke und ihre Auswirkung auf die Unternehmenssicherheit" Studie mit der Hochschule Augsburg 2012, Seite 3

[2] Bernhard Meuser: „Youcat und THINC!, Neuevangelisierung mit dem Jugendkatechismus", Augsburg 2012

[3] BITKOM: „Soziale Netzwerke, repräsentative Untersuchung zur Nutzung sozialer Netzwerke im Internet" 2011

[4] BITKOM: a.a.O

1. Datenschutz

1.1 „social-Plug-ins" und „Like-Button"

Nach einer Erhebung des VDD (Verband der Diözesen Deutschlands) im Dezember 2011 hat die Mehrzahl der Deutschen Diözesen den „Facebook Like-Button" oder wenigstens „Facebook" als sog. „social-Plug-in" (automatisierte Verlinkung von der Homepage des Bistums auf die „Facebook-Fanpage") in die jeweilige Bistumshomepage eingebunden. Aus datenschutzrechtlicher Sicht ist dies bedenklich, da bereits beim Laden der jeweiligen Bistumsseite, in die der „Like-Button" eingebunden ist, Daten des Besuchers der Seite (wenigstens die IP-Adresse des PC) ohne dessen aktives Zutun an die Betreiber der Netzwerkplattformen (hier „Facebook") übertragen werden. Die ständige Arbeitsgruppe Datenschutz-und Melderecht/IT-Recht der Rechtskommission des VDD hat daher einen vollständigen Verzicht auf das Einbinden des „Like-Buttons" empfohlen. Für den Fall, dass der „Like-Button" dennoch eingebunden bleiben soll, wird empfohlen, wenigstens die sog. 2klick-Lösung von Heise zu verwenden. Damit wird sichergestellt, dass der „Like-Button" zwar eingebunden, aber regelmäßig deaktiviert ist und erst nach einem weiteren, bewussten Klick aktiviert wird, Daten damit nur mit Zustimmung des Anwenders an „Facebook" übertragen werden[5].
Auch im Falle der 2klick-Lösung von Heise muss allerdings zwingend der Besucher der Bistumshomepage im Rahmen einer Datenschutzerklärung von der Datenübertragung in Kenntnis gesetzt werden, da nach einem Beschluss des „Düsseldorfer Kreises" (Zusammenschluss der obersten deutschen Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich) vom 08. Dezember 2011 *„Voraussetzung für eine wirksame Zustimmung* (also den zweiten Klick) *ist, dass der Webseitenbetreiber* (hier das Bistum) *darüber informiert, welche Daten zu welchem Zweck an den Netzwerkbetreiber* (hier „Facebook")" übermittelt werden. Dies gilt im Besonderen dann, wenn der Besucher selbst ein „Facebook-Profil" hat. Eine solche Datenschutzerklärung könnte z.B. folgenden Inhalt haben:

Datenschutzerklärung für die Nutzung von „Facebook"-Plug-ins (Like-Button)

Auf unseren Seiten sind Plug-ins des sozialen Netzwerks „Facebook", 1601 South California Avenue, Palo Alto, CA 94304, USA integriert. Die „Facebook"-Plug-ins erkennen Sie an dem „Facebook"-Logo oder dem "Like-Button" ("Gefällt mir") auf unserer Seite. Eine Übersicht über die „Facebook"-Plug-ins finden Sie hier: http://developers."Facebook".com/docs/plugins/ Wenn Sie unsere Seiten besuchen, wird über das Plug-in eine direkte Verbindung zwischen Ihrem Browser und dem „Facebook"-Server hergestellt. „Facebook" erhält dadurch die Information, dass Sie mit Ihrer IP-Adresse unsere Seite besucht haben. Wenn Sie den „Facebook" „Like-Button" anklicken, während Sie in Ihrem „Facebook"-Konto eingeloggt sind, können Sie die Inhalte unserer Seiten auf Ihrem „Facebook"-Profil verlinken. Dadurch kann „Facebook" den Besuch unserer Seiten Ihrem Benutzerkonto zuordnen. Wir weisen darauf hin, dass wir als Anbieter der Seiten keine Kenntnis vom Inhalt der übermittelten Daten sowie deren Nutzung durch „Facebook" erhalten. Weitere Informationen hierzu finden Sie in der Datenschutzerklärung von „Facebook" unter http://de-de."Facebook".com/policy.php. Wenn Sie nicht wünschen, dass „Facebook" den Besuch unserer Seiten Ihrem „Facebook"-Nutzerkonto zuordnen kann, loggen Sie sich bitte aus Ihrem „Facebook"-Benutzerkonto aus.[6]

Die gleiche Empfehlung richtet sich auch an die pfarrlichen Nutzer von „Facebook-Fanpages".

---

[5] http://www.heise.de/newsticker/meldung/code-fuer-2-klick-empfehlungsbutton-von-heise-ist-erhaeltlich-1337833.html

[6] Facebook-Disclaimer von eRecht24.de

1.2. „Facebook" Datenschutzrichtlinien/Datenverwendungsrichtlinien

Nahezu zeitgleich mit dem Gang zur Börse hat „Facebook" seine „Datenschutzrichtlinien" in „Datenverwendungsrichtlinien" umbenannt und diese um eine Fülle von Personalisierungsmöglichkeiten für Werbekunden erweitert. Schon die geänderte Begrifflichkeit lässt aufhorchen. „Facebook" dokumentiert damit, dass der Schutz der personenbezogenen Daten mit dem Börsengang gegenüber der Verwendung personenbezogener Daten (durch „Facebook" und seine Werbekunden) nachrangig ist. Im Besonderen bedenklich ist dabei das „Facebook"-Programm der „umgehenden Personalisierung".[7]

Nimmt ein „Partner" („Facebook"-Werbekunde) am „Facebook"-Programm zur umgehenden Personalisierung" teil und hat der Betroffene in seinem persönlichen „Facebook"-Profil die sofortige Personalisierung nicht deaktiviert, so werden auf der Homepage des Partners bei dessen Besuch des Betroffenen die Nutzerdaten des Betroffenen „sofort personalisiert". Dies bedeutet nach eigener Angabe in den „Datenverwendungsrichtlinien", dass „Facebook" dem Partner die „Facebook"-Nutzerkennnummer einschl. der Altersgruppe, des Standorts und des Geschlechts des Betroffenen sowie dessen Freundesliste (ohne deren Wissen und Wollen!) übermittelt. Weiter wird dem Partner erlaubt, auf die öffentlichen Daten des Betroffenen und seiner „Freunde" über „Facebook" zuzugreifen, um zielgerichtet Werbung bereitzustellen. „Facebook" begründet diesen Vorgang folgendermaßen: *„… um sowohl auf als auch außerhalb von „Facebook" ein noch persönlicheres und umfeldorientierteres Nutzungserlebnis für angemeldete Nutzer als bei einem sozialen Plug-in zu ermöglichen."*[8]

Bei „Facebook" ist die „umgehende Personalisierung" standardmäßig auf „ein" gestellt und „Facebook" macht seinen Nutzern eine Deaktivierung dieser Einstellung nicht einfach. Erst nach dem „Durchklicken" von sechs Menüpunkten in seinen Privatsphäre-Einstellungen (siehe Schaubild auf den Folgeseiten) findet der User das Kontrollkästchen und wird beim Deaktivierungsvorgang sogar noch „gewarnt", diesen auszuführen. Wesentlich datenschutz- und benutzerfreundlicher wäre es, wenn das Kontrollkästchen standardmäßig auf „aus" gestellt wäre. „Facebook" hat die Einstellungen für die Privatsphäre in jüngster Zeit auch mehrfach (ohne Ankündigung oder Hinweise) verändert. So findet sich die Einstellung zur „umgehenden Personalisierung" mittlerweile in den Privatsphäre-Einstellungen unter „Apps". In den Hilfeeinstellungen wird der User allerdings hierbei noch auf die nicht mehr aktiven Einstellungsmöglichkeiten hingewiesen.

[7] Facebook Site Governance vom 15.11.2013, III. Andere Webseiten und Anwendungen, Über die sofortige Personalisierung

[8] Facebook Site Governance vom 15.11.2013, a.a.O

Wie funktioniert die umgehende Personalisierung auf Drittanbieter-Webseiten?

Mit der umgehenden Personalisierung kannst du deine Freunde und Interessenten mitnehmen, wenn du eine Anwendung oder Webseite besuchst. Anwendungen und Webseiten, die diese Funktion nutzen, müssen sich an eindeutige Datenschutzrichtlinien halten und dürfen nur die Informationen in deinem öffentlichen Profil und deine Freundesliste verwenden, um dir eine individuellere Nutzererfahrung zu bieten.

Wenn du eine Webseite zum ersten Mal unter Verwendung der umgehenden Personalisierung besuchst, wird dir eine Benachrichtigung darüber angezeigt, dass dein Nutzererlebnis personalisiert wird, wenn du bei Facebook angemeldet bist. Du kannst dann mehr dazu erfahren oder das personalisierte Nutzererlebnis ablehnen, indem du auf „**Deaktivieren**" klickst.

Wenn du keine Personalisierung auf diesen Seiten wünschst, kannst du die umgehende Personalisierung vollständig deaktivieren:

1. Klicke in Facebook auf ⚙, und wähle „**Privatsphäre-Einstellungen**".
2. Klicke im Bereich „**Werbeanzeigen, Anwendungen und Webseiten**" auf „**Einstellungen bearbeiten**".
3. Dort kannst du deine Einstellungen im Bereich „**Umgehende Personalisierung**" bearbeiten.

„Anleitung" im „Facebook" Hilfebereich zur Deaktivierung der „umgehenden Personalisierung", nur…:

diesen Bereich gibt es in den Privatsphäre-Einstellungen gar nicht mehr!

Die AGB von „Facebook" gehören zu den am meisten kritisierten AGBs aller sozialen Netzwerke. Diese beinhalten u.a. die Klausel, dass für „Inhalte, die unter die Rechte an geistigem Eigentum fallen, wie Fotos und Videos ... vorbehaltlich ... der ... Privatsphäre- und Anwendungseinstellungen ... die folgende Erlaubnis erteilt wird: Ein Benutzer überträgt „Facebook" ... eine nicht-exklusive, übertragbare, unterlizenzierbare, unentgeltliche, weltweite Lizenz für die Nutzung jeglicher ... Inhalte der genannten Art, die ... auf oder im Zusammenhang mit „Facebook" ... gepostet werden". Dies schließt unter anderem das Recht ein, persönliche Daten von Usern an Dritte zu verkaufen.[9]

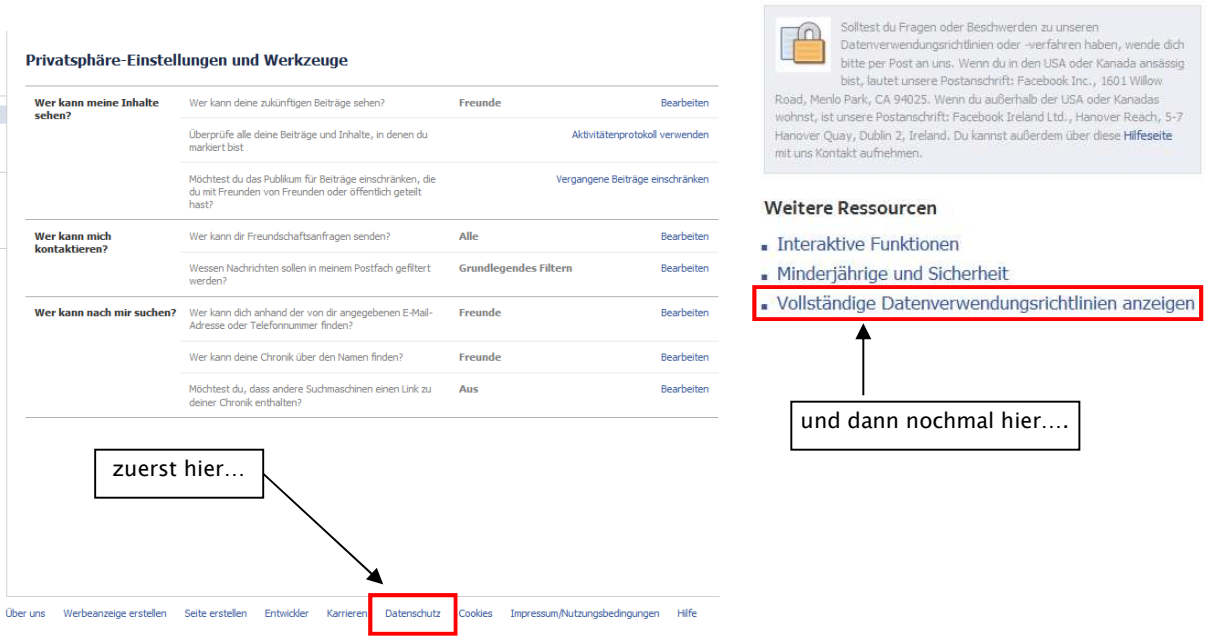
Der Umgang mit Daten bei „Facebook" verteilt sich auf drei Ebenen. Die tiefste Ebene bildet der riesige Pool, in den unaufhörlich neue Daten fließen. Dieses Rohmaterial veredelt „Facebook" auf einer zweiten Ebene, indem es mit unbekannten Techniken Verknüpfungen erstellt, Beziehungen der Subjekte bildet, clustert und Interessenlagen der Mitglieder auswertet. All das entzieht sich dem Einfluss, ja sogar der Kenntnis der Nutzer. Erst auf der dritten Ebene, also dort, wo die Kommunikation zwischen den Nutzern läuft, gewährt „Facebook" Eingriffsmöglichkeiten in Form von Privatsphäre-Optionen. Kurz gesagt: Der Nutzer darf Informationen gegenüber anderen Nutzern, nicht aber gegenüber „Facebook" unterdrücken.[10]

Gerechterweise muss gesagt werden, dass „Facebook" in seinen Nutzungs- und in den Datenverwendungsrichtlinien mittlerweile darauf hinweist, was es mit den Daten seiner Nutzer beabsichtigt. Die Datenverwendungsrichtlinien sind dabei allerdings insgesamt so komplex und umfangreich gestaltet, dass kaum ein User, besonders nicht Minderjährige, sie wirklich vollständig lesen (und auch verstehen) werden, um dann persönliche Entscheidungen zu den Privatsphäre-Einstellungen treffen zu können. Schon das bloße Auffinden der vollständigen Datenverwendungsrichtlinien ist nicht einfach. Der interessierte Nutzer muss

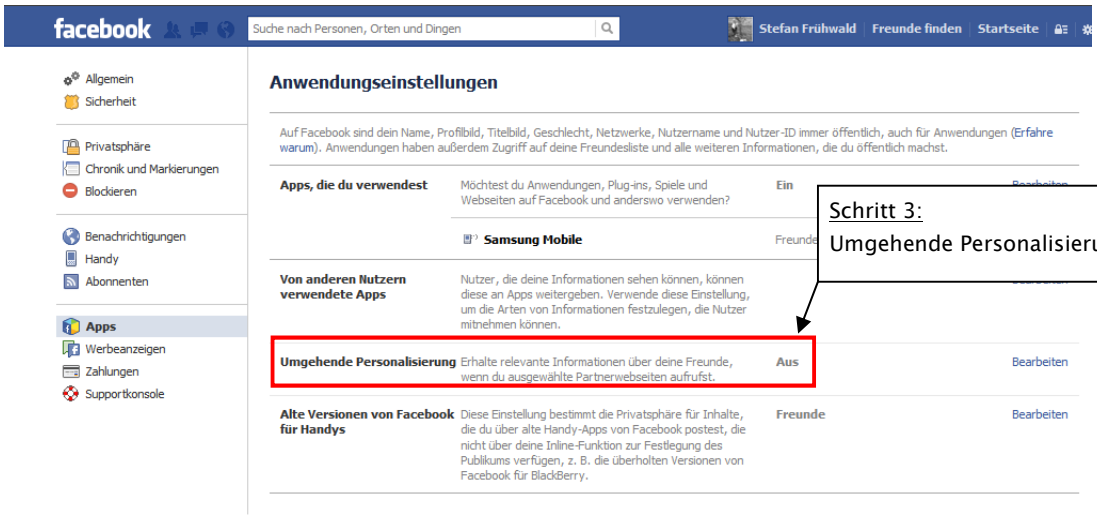
[9] Bayerisches Landesamt für Verfassungsschutz: „Soziale Netzwerke und ihre Auswirkung auf die Unternehmenssicherheit" Studie mit der Hochschule Augsburg 2012, Seite 21

[10] Holger Bleich in: „Des Nutzers neue Kleider", www.ct.de/1122098

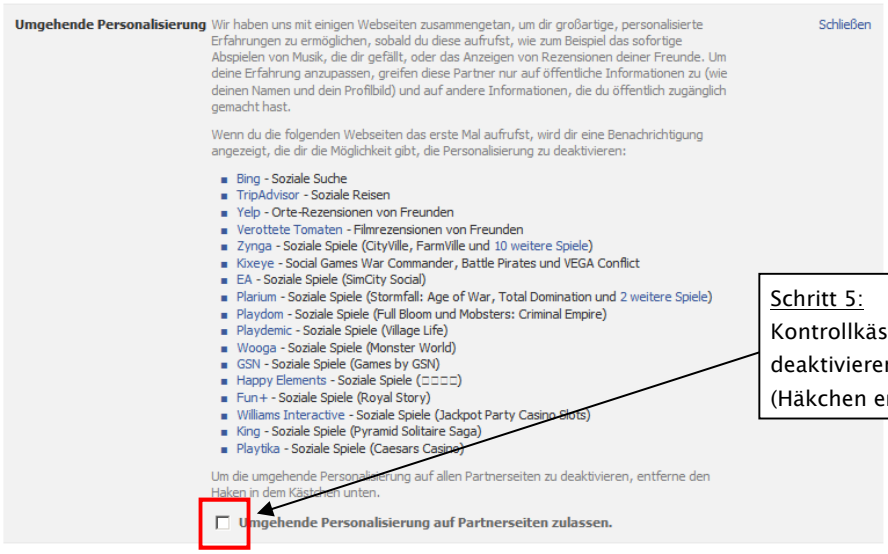
dazu über die Privatsphäre-Einstellungen am unteren Rand auf „Datenschutz“ und danach nochmal auf „vollständige Datenverwendungsrichtlinien anzeigen“ klicken.



Darstellung des Deaktivierungsvorgangs „umgehende Personalisierung“


facebook
Suche nach Personen, Orten und Dingen
Stefan Frühwald
Freunde finden
Startseite
Allgemein
Sicherheit
Privatsphäre
Chronik und Markierungen
Blockieren
Benachrichtigungen
Handy
Abonnenten
Apps
Werbeanzeigen
Zahlungen
Supportkonsole
Anwendungseinstellungen
Auf Facebook sind dein Name, Profilbild, Titelbild, Geschlecht, Netzwerke, Nutzername und Nutzer-ID immer öffentlich, auch für Anwendungen (Erfahre warum). Anwendungen haben außerdem Zugriff auf deine Freundesliste und alle weiteren Informationen, die du öffentlich machst.
Apps, die du verwendest
Möchtest du Anwendungen, Plug-ins, Spiele und Webseiten auf Facebook und anderswo verwenden?
Ein
Bearbeiten
Samsung Mobile
Freunde
Von anderen Nutzern verwendete Apps
Nutzer, die deine Informationen sehen können, können diese an Apps weitergeben. Verwende diese Einstellung, um die Arten von Informationen festzulegen, die Nutzer mitnehmen können.
Umgehende Personalisierung
Erhalte relevante Informationen über deine Freunde, wenn du ausgewählte Partnerwebseiten aufrufst.
Aus
Bearbeiten
Alte Versionen von Facebook für Handys
Diese Einstellung bestimmt die Privatsphäre für Inhalte, die du über alte Handy-Apps von Facebook postest, die nicht über deine Inline-Funktion zur Festlegung des Publikums verfügen, z. B. die überholten Versionen von Facebook für BlackBerry.
Freunde
Bearbeiten
Schritt 3:
Umgehende Personalisierung


Informationen zur umgehenden Personalisierung
So, wie in deinen Neuigkeiten die Personen und Dinge angezeigt werden, die dich interessieren, hilft dir die umgehende Personalisierung dabei, Freunde und interessante Inhalte auf anderen Webseiten zu finden. Wir haben uns mit einigen Unternehmen wie Pandora und TripAdvisor zusammengetan, um diese Webseiten unterhaltsamer und nützlicher gestalten, sobald du sie aufrufst.
Mehr dazu
With Paul WS Anderson
FRIENDS ACTIVITY
Schließen
Schritt 4:
Werbevideo für die umgehende Personalisierung schließen


Umgehende Personalisierung
Wir haben uns mit einigen Webseiten zusammengetan, um dir großartige, personalisierte Erfahrungen zu ermöglichen, sobald du diese aufrufst, wie zum Beispiel das sofortige Abspielen von Musik, die dir gefällt, oder das Anzeigen von Rezensionen deiner Freunde. Um deine Erfahrung anzupassen, greifen diese Partner nur auf öffentliche Informationen zu (wie deinen Namen und dein Profilbild) und auf andere Informationen, die du öffentlich zugänglich gemacht hast.
Schließen
Wenn du die folgenden Webseiten das erste Mal aufrufst, wird dir eine Benachrichtigung angezeigt, die dir die Möglichkeit gibt, die Personalisierung zu deaktivieren:
Bing - Soziale Suche
TripAdvisor - Soziale Reisen
Yelp - Orte-Rezensionen von Freunden
Verottete Tomaten - Filmrezensionen von Freunden
Zynga - Soziale Spiele (CityVille, FarmVille und 10 weitere Spiele)
Kixeye - Social Games War Commander, Battle Pirates und VEGA Conflict
EA - Soziale Spiele (SimCity Social)
Plarium - Soziale Spiele (Stormfall: Age of War, Total Domination und 2 weitere Spiele)
Playdom - Soziale Spiele (Full Bloom und Mobsters: Criminal Empire)
Playdemic - Soziale Spiele (Village Life)
Wooga - Soziale Spiele (Monster World)
GSN - Soziale Spiele (Games by GSN)
Happy Elements - Soziale Spiele (□□□□)
Fun+ - Soziale Spiele (Royal Story)
Williams Interactive - Soziale Spiele (Jackpot Party Casino Slots)
King - Soziale Spiele (Pyramid Solitaire Saga)
Playtika - Soziale Spiele (Caesars Casino)
Um die umgehende Personalisierung auf allen Partnerseiten zu deaktivieren, entferne den Haken in dem Kästchen unten.
Umgehende Personalisierung auf Partnerseiten zulassen.
Schritt 5:
Kontrollkästchen deaktivieren (Häkchen entfernen)

„Facebook“ beabsichtigt, in Kürze seine überarbeiteten Nutzungsbedingungen vor allem hinsichtlich der Verwendung von Nutzer-Daten zu Werbezwecken in Kraft zu setzen. In der gültigen Fassung heißt es unter Punkt 10: *„Du kannst über deine Privatsphäre-Einstellungen einschränken, inwiefern dein Name und dein Profilbild mit kommerziellen, gesponserten oder verwandten Inhalten (wie z.B. der Marke, die dir gefällt) verbunden werden können, die von uns zur Verfügung gestellt oder aufgewertet werden. Du erteilst uns die Erlaubnis, vorbehaltlich der von dir festgelegten Einschränkungen, deinen Namen und dein Profilbild in Verbindung mit diesen Inhalten zu verwenden.“* Der Nutzer kann also, wenn auch nur für seinen Namen und sein Profilbild, Einstellungen vornehmen, die eine Weitergabe an Werbetreibende einschränken. Diese Einschränkung möchte „Facebook“ nun nicht mehr gelten lassen. In den neuen Nutzungsbedingungen heißt es jetzt: *„Du erteilst uns deine Erlaubnis zur Nutzung deines Namens, Profilbilds, deiner Inhalte und Informationen im Zusammenhang mit kommerziellen, gesponserten oder verwandten Inhalten (z.B. eine Marke, die dir gefällt), die von uns zur Verfügung gestellt oder aufgewertet werden. Dies bedeutet beispielsweise, dass du einem Unternehmen bzw. einer sonstigen Organisation die Erlaubnis erteilst, uns dafür zu bezahlen, deinen Namen und/oder dein Profilbild zusammen mit deinen Inhalten oder Informationen ohne irgendeine Entlohnung für dich zu veröffentlichen. Wenn du eine bestimmte Zielgruppe für deine Inhalte oder Informationen ausgewählt hast, werden wir deine Auswahl bei deren Nutzung respektieren.*

Solltest du jünger als achtzehn (18) Jahre alt sein bzw. gemäß einer anderen gesetzlichen Altersgrenze als minderjährig gelten, versicherst du, dass mindestens ein Elternteil bzw. Erziehungsberechtigter den Bedingungen dieses Abschnitts (sowie der Verwendung deines Namens, Profilbilds, deiner Inhalte und Informationen) in deinem Namen zugestimmt hat.“

Laut „Facebook“ sei damit lediglich beabsichtigt, die Erlaubnis, dass „Facebook“ Daten seiner Nutzer zu Werbezwecken verwendet, klarer und verständlicher zu fassen. „Facebook“ erteilt

sich damit aber generell die Erlaubnis, grundsätzlich alle Daten seiner User gewinnbringend zu vermarkten. Erschwerend kommt hinzu, dass auch und gerade die Rechte Minderjähriger und ihrer Erziehungsberechtigten nahezu „ausgehebelt" werden. „Facebook" geht davon aus, dass schon durch die bloße Nutzung seiner Dienste, und nicht erst durch ausdrückliches Akzeptieren der Nutzungsbedingungen, die Zustimmung der Erziehungsberechtigten zur Datenweitergabe erteilt ist. Nach einer Bewertung europäischer und mittlerweile sogar einiger US-amerikanischer Datenschützer verstößt „Facebook" mit den neuen Nutzungsbedingungen gegen das Abkommen mit der US-Handelsbehörde FTC (Federal Trade Comission) aus dem Jahr 2011.[11]

1.3. EU-Datenschutzverordnung, „Recht auf Vergessenwerden und auf Löschung"

Artikel 17 des Entwurfs der neuen EU-Datenschutzverordnung *garantiert dem Betroffenen das Recht, vergessen zu werden, sowie das Recht auf Löschung. Das in Artikel 12 b der Richtlinie 95/46/EG geregelte Recht auf Löschung wird weiter ausgeführt und präzisiert einschließlich der Bedingungen für das Recht auf Vergessenwerden. Hierzu zählt auch die Pflicht des für die Verarbeitung Verantwortlichen, der die personenbezogenen Daten veröffentlicht hat, Dritte über den Antrag der betroffenen Person auf Löschung aller Verbindungen zu diesen personenbezogenen Daten oder auf Löschung von Kopien oder Replikationen dieser Daten zu informieren. Darüber hinaus wird ein Recht auf Beschränkung der Datenverarbeitung in bestimmten Fällen eingeführt.*[12]
Diesem „Recht auf Vergessenwerden" widersprechen die erst jüngst, zuletzt am 15.11.2013 geänderten „Facebook-Datenverwendungsrichtlinien" eklatant: *„Wir können das Konto einer verstorbenen Person in den Gedenkzustand versetzen. Wenn wir ein Konto in den Gedenkzustand versetzen, bleibt die betreffende Chronik auf „Facebook" bestehen; allerdings schränken wir den Zugriff und einige Funktionen ein. Wir können ein Konto auch schließen, wenn wir eine formelle Aufforderung erhalten, die bestimmte Kriterien erfüllt*

„Facebook" lässt offen, welche „bestimmten" Kriterien für ein Schließen des Kontos erfüllt sein müssen. Auch bedeutet „Schließen" bei „Facebook" keineswegs „Löschen", da „Facebook" an anderer Stelle in den neuen Datenverwendungsrichtlinien ausdrücklich zwischen „Löschen" und „Deaktivieren" differenziert.[13] „Schließen" meint folglich nur, dass das Konto einer verstorbenen Person nicht mehr öffentlich sichtbar ist, die gespeicherten Daten bleiben allerdings für „Facebook" selbst weiterhin verfügbar.

Zwar stellt „Facebook" mittlerweile ein Formular zur Verfügung, um das Konto einer verstorbenen Person auch endgültig löschen zu können, verzichtet aber leider in seinen Datenverwendungsrichtlinien auf einen entsprechenden textlichen Hinweis. Der in den Datenverwendungsrichtlinien enthaltene Link https://www.facebook.com/help/contact.php?show_form=deceased führt den Nutzer lediglich zu einem Antragsformular, das Konto in den „Gedenkzustand"

---

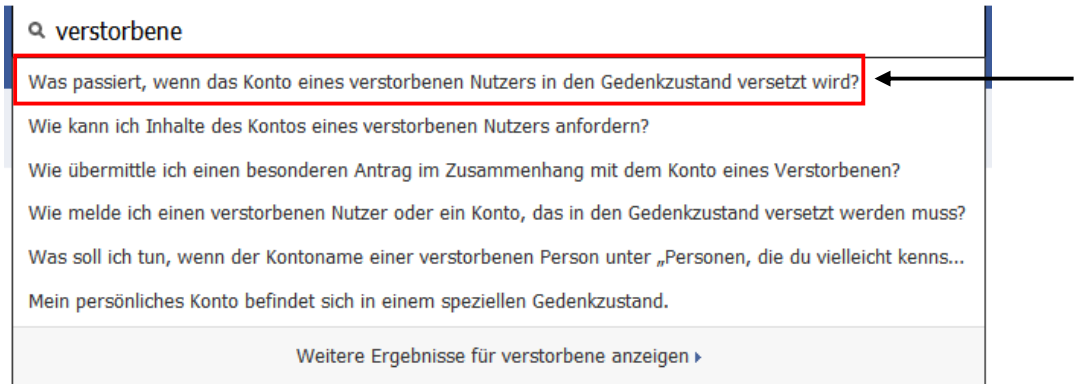
[11] spiegel-online vom 05.09.2013, www.spiegel.de/netzwelt/web/datenschutz-facebook-aendert-die-nutzungsbedingungen-a-920519.html

[12] EU-Datenschutzverordnung, Vorschlag der Kommission vom 25.01.2012, Seite 10, 3.4.3.3. Abschnitt 3 – Berichtigung und Löschung

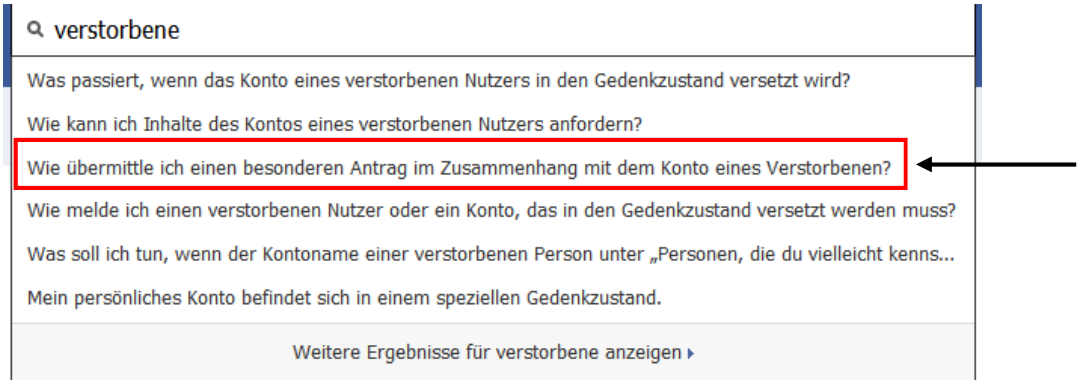
[13] Facebook Site Governance vom 15.11.2013, I. Daten, die wir erhalten und ihre Verwendung, Löschung und Deaktivierung deines Kontos

zu versetzen. Um das Antragsformular zur Löschung des Kontos einer verstorbenen Person zu finden, muss sich der Nutzer tiefer in den Hilfebereich von „Facebook“ begeben und schon etwas genauer mit den „Facebook“-spezifischen Begrifflichkeiten vertraut sein. Gibt eine betroffene Person in der Suchfunktion des Hilfebereichs den Begriff „Verstorbene – Konto – löschen“ ein, so führt dies zunächst zu keinem Ergebnis.

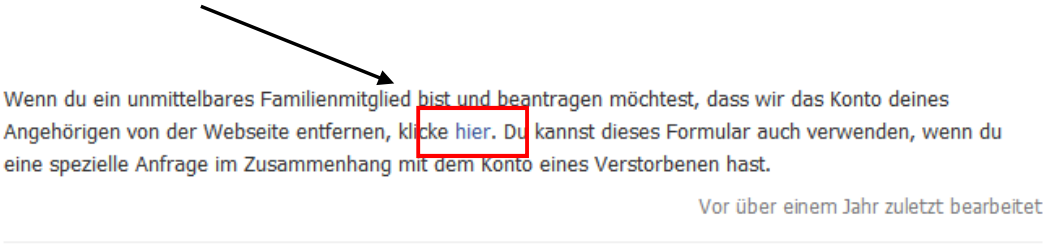
Und auch mit der bloßen Eingabe „Verstorbene“ im Suchfeld wird die betroffene Person in erster Linie wieder auf den „Gedenkzustand“ verwiesen.



Erst das Anklicken von „Wie übermittle ich einen besonderen Antrag im Zusammenhang mit dem Konto eines Verstorbenen“ führt eine betroffene Person zu allgemeinen Erläuterungen und letztlich dann über einen weiteren Link zum „besonderen Antragsformular“[14].



Wie sollte aber eine „Facebook“ eher unkundige Person wissen, dass sich der Link zu diesem „besonderen Antragsformular“ ganz am Ende der allgemeinen Erläuterungen hinten einem kleinen, blauen „hier“ verbirgt?

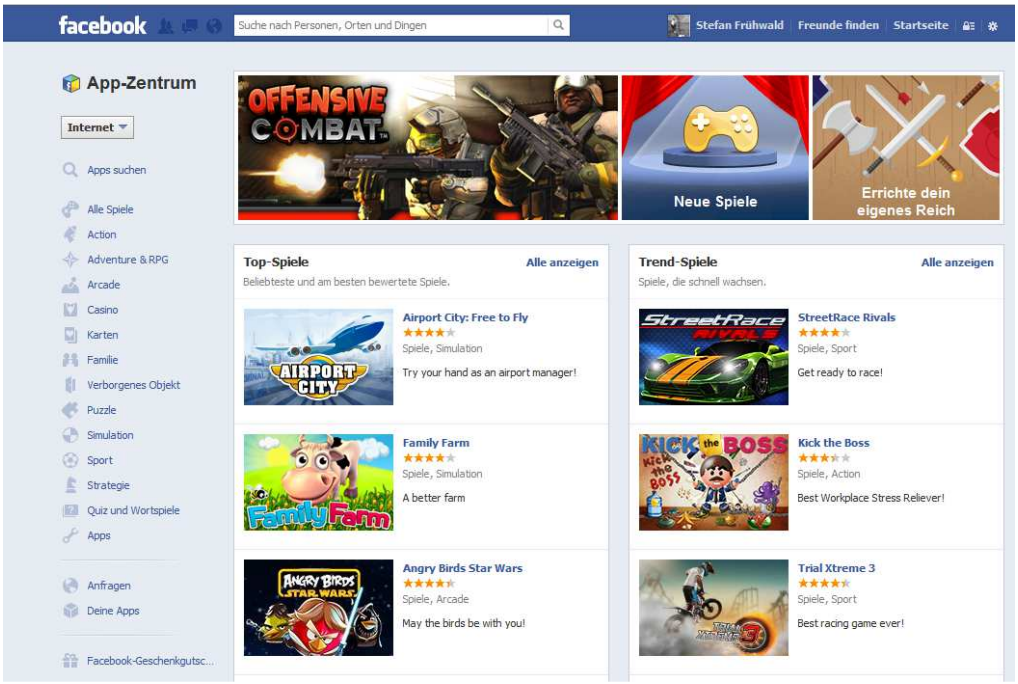


Dem Recht auf Löschung nach Art. 17 des Entwurfs der EU-Datenschutzverordnung, im Besonderen für personenbezogene Daten, die der Betroffene im Kindesalter öffentlich gemacht hat, kommt „Facebook“ nur scheinbar mit der Möglichkeit der Löschung des Kontos nach. „Facebook“ weist darauf hin, dass: *„… einige Dinge, die du auf „Facebook“ machst, nicht in deinem Konto gespeichert werden…. Solche Informationen bleiben auch nach der Löschung erhalten.“*[15] Letztlich führt dies die Löschung eines Kontos ad absurdum, da schon nach kurzer Nutzungszeit eines „Facebook-Kontos“ in den Konten der „Freunde“ nahezu sämtliche persönlichen Daten eines „Freundes“ durch Postings, „Teilen“ von Nachrichten und Inhalten etc. gespeichert sind und folglich auch nach dem Löschen dort gespeichert und für „Facebook“ verfügbar bleiben. Auch scheint „Facebook“ das Löschen eines Kontos nur ungenügend auszuführen, denn: *„Was ist dann davon zu halten, dass im Profil eines unserer Kollegen, der aus „Facebook“-Überdruss alle seine Postings gelöscht hatte, nach drei Wochen ebendiese plötzlich für seine Freunde wieder sichtbar wurden?“*[16]

[14] http://de-de.facebook.com/help/contact/228813257197480
[15] Facebook Site Governance vom 15.11.2013, a.a.O. (Fußnote 11)
[16] Holger Bleich in: „Des Nutzers neue Kleider“, www.ct.de/1122098

Bemerkenswert ist auch noch, dass der Nutzer sein Konto zwar über die Kontoeinstellungen deaktivieren kann, die Funktion, das Konto „endgültig“ zu löschen, allerdings nur über einen Link an versteckter Stelle in den Hilfeseiten findet[17].

Kritisch zu sehen ist ferner das Verhältnis von „Facebook“ zu externen Anwendungen. Dabei handelt es sich um Spiele, Ratgeber, Horoskope etc., die unmittelbar über das „Facebook-Konto“ geladen und ausgeführt werden. Zwar kann der Nutzer diese externen Anwendungen wieder aus seinem Konto entfernen bzw. sogar in den Privatsphäre-Einstellungen die Ausführung generell unterbinden, doch können diese Anwendungen auch weiterhin Zugriff auf die Nutzerdaten haben. „Facebook“ lässt in seinen Datenverwendungsrichtlinien offen, ob und welche Nutzerdaten von externen Anwendungen auch nach dem Löschen der jeweiligen Anwendung gespeichert bleiben und verweist den Nutzer lediglich darauf, *„die Anwendung selbst zu kontaktieren und um Löschung zu bitten“*.[18] *„Der Nutzer soll also nach Vorstellung von „Facebook“ selbst aktiv werden. „Facebook“ sieht sich selbst nicht in der Pflicht dafür zu sorgen, dass Anwendungen sich an die Datenverwendungsrichtlinien von „Facebook“ auch tatsächlich halten.“*[19]



Beispiel für externe Anwendungen

Aktuell ist „Facebook“ in Europa mit einer ganzen Reihe von Anzeigen von Datenschützern vor der irischen Datenschutzaufsichtsbehörde konfrontiert[20]:

*(1) **Pokes (Anstupsen):** Die Daten werden nach dem “Entfernen” von „Facebook“ weiter gespeichert und nie wieder gelöscht.*

[17] Bayerisches Landesamt für Verfassungsschutz: „Soziale Netzwerke und ihre Auswirkung auf die Unternehmenssicherheit“ Studie mit der Hochschule Augsburg 2012, Seite 20

[18] Facebook Site Governance vom 15.11.2013, III. Andere Webseiten und Anwendungen, Kontrolle, welche deiner Daten Anwendungen bereitgestellt werden.

[19] Zeit-online vom 18.05.2012, „Facebook verdeutlicht die eigenen Mängel“

[20] Fraunhofer SIT Technical Reports SIT-TR-2013-02 „soziale Netzwerke bewusst nutzen“, 2.1.1 unrechtmäßige Datensammlung

*(2) **Schattenprofile**: „Facebook“ sammelt im Hintergrund Daten von Personen, ohne dass der Betroffene dies bemerkt oder dem zustimmt. Betrifft vor allem Personen ohne „Facebook“.*

*(3) **Markieren**: Markierungen werden ohne Zustimmung des Users (Opt-In) aktiviert. Der User muss die Daten dann entfernen (Opt-Out).*

*(4) **Synchronisieren**: „Facebook“ saugt persönliche Daten z. B. mittels iPhone-App oder E-Mail-Import ab und verwendet diese Daten für seine eigenen Zwecke – ohne die Zustimmung des Betroffenen.*

*(5) **Gelöschte Postings**: Postings auf den Seiten der „Facebook“nutzer werden auch nach dem “Entfernen” weiter gespeichert.*

*(6) **Postings auf fremden Seiten**: Der User kann nicht herausfinden, wer seine auf fremden Seiten hinterlassenen Daten sehen kann.*

*(7) **Messages**: Nachrichten (inkl. Chat-Nachrichten) werden auch nach dem “Löschen” weiter gespeichert. Damit wird die gesamte direkte Kommunikation auf „Facebook“ dauerhaft unlöschbar.*

*(8) **Datenschutzbestimmungen und Zustimmung**: Die Datenschutzbestimmungen sind vage, unklar und widersprüchlich. Nach europäischen Standards ist die Zustimmung ungültig.*

*(9) **Gesichtserkennung**: Die neue Gesichtserkennung (in Europa derzeit inaktiv) ist ein unverhältnismäßiger Eingriff in die Privatsphäre der Nutzer. Außerdem fehlen Hinweise und die Zustimmung.*

*(10) **Auskunft mangelhaft**: Die Auskunft, zu welcher „Facebook“ gesetzlich verpflichtet ist, ist in vielen Punkten mangelhaft. Viele Daten und Informationen fehlen.*

*(11) **Löschen von Markierungen**: Markierungen (z. B. in Fotos), die “entfernt” werden, werden von „Facebook“ nur deaktiviert.*

*(12) **Datensicherheit**: „Facebook“ sagt in seinen Nutzungsbedingungen, dass es nicht sicherstellen kann, dass Daten sicher sind.*

*(13) **Anwendungen**: Anwendungen von Freunden können auf die Daten des Nutzers zugreifen. Es gibt keine entsprechenden Sicherheiten, dass die Anwendungen europäischen Datenschutzstandards entsprechen.*

*(14) **Gelöschte Freunde**: Freunde, die gelöscht werden, bleiben weiter auf „Facebook“ gespeichert.*

*(15) **Exzessive Datennutzung**: „Facebook“ sammelt unglaubliche Datenmengen als “Host”, die eigene Nutzung ist unlimitiert.*

*(16) **Opt-Out**: Die Verwendung der Daten auf „Facebook“ ist faktisch “Opt-Out” statt “Opt-In”, das widerspricht den europäischen Gesetzen.*

*(17) **Like-Button**: Der von „Facebook“ derzeit angebotene “Like-Button” ist nicht datenschutzkonform und kann zum Ausspionieren der Nutzer verwendet werden.*

*(18) **Pflichten als Auftragsverarbeiter**: „Facebook“ hat gegenüber den Nutzern die Pflicht, die vom Nutzer auf „Facebook“ hinterlegten Daten nicht für eigene Zwecke zu missbrauchen.*

*(19) **Privatsphäre-Einstellungen bei Bildern**: Die User können nur steuern, wer den Link zu einem Bild sehen kann. Das Bild selbst ist für jeden abrufbar, der den Link kennt. Es gibt keine wirkliche Steuerung über Zugriffsrechte.*

*(20) **Gelöschte Bilder**: Gelöschte Bilder sind weiter abrufbar und werden erst mit großer Verzögerung gelöscht. Nur der Link zum Bild auf „Facebook".com wird unsichtbar.*

*(21) **Gruppenmitgliedschaft**: Nutzer können ohne ihre Zustimmung zu Gruppen hinzugefügt werden und müssen dann aktiv wieder austreten.*

*(22) **Änderung der Datenschutzrichtlinien**: Datenschutzbestimmungen werden regelmäßig ohne entsprechende Information und Zustimmung der User geändert.*

1.4 Daten von Nicht-Mitgliedern

Auch wer gar kein „Facebook-Konto", sondern vielleicht nur eine E-Mail Adresse hat, muss „Facebook" noch lange nicht unbekannt bleiben. Mit der „Freunde-Finder" Funktion drängt „Facebook" seine Mitglieder dazu, Adressbücher von Telefonen und E-Mail-Konten nach „Facebook" hochzuladen, vorgeblich nur, um Bekannte bei „Facebook" zu finden oder diejenigen Bekannten zu „Facebook" einzuladen, die dort noch kein Konto haben. „Facebook-Nutzer", die dies nicht möchten, müssen die Funktion durch eine eigene, wiederum vergleichsweise aufwändige Aktion ausschalten.[21] Tun sie dies nicht, speichert „Facebook" die Adressdaten von Nicht-Mitgliedern (und zwar ohne deren Einverständnis!) aus den Adressbüchern seiner Mitglieder nach dem Hochladen wenigstens zwei Monate lang, um diesen eine Erinnerungs-E-Mail an die Einladung zuzusenden. Zwar hat das Landgericht Berlin in jüngster Entscheidung (LG Berlin, Urt. vom 06.03.2012 -16 O 551/10) die bisherige, nahezu automatisierte Praxis von „Facebook" zum „Freunde finden und einladen" bereits beim Registrierungsvorgang als unlauter gewertet, allerdings verweist die Literatur darauf, dass ein geänderter „Freunde-Finder-Prozess" sehr wohl zulässig sein könnte[22]. Dies wäre z.B. dann der Fall, wenn Absender der „Einladungs-E-Mail" nicht „Facebook", wie bisher, sondern der Nutzer selbst wäre. „Facebook" hat gegen das Urteil Revision eingelegt.

Eine weitere Möglichkeit, über „Facebook" Daten von Nicht-Mitgliedern zu erhalten, ist eine Smartphone-Anwendung, die von „Facebook"-Nutzern verwendet werden kann. Dabei synchronisiert der User seine Smartphone-Kontakte mit seinen „Facebook"-Freunden und „Facebook" kann dadurch Informationen wie Namen, Telefonnummern, E-Mail-Adressen und Geburtstage von Nicht-Mitgliedern speichern. Inzwischen wird von „Facebook" ein Kontaktformular angeboten, das es nicht im sozialen Netzwerk registrierten Personen ermöglicht, alle Daten, die mit ihrer E-Mail-Adresse verknüpft sind, löschen zu lassen. Dies erzielt allerdings nur dann den gewünschten Effekt, wenn „Facebook" bereits eine Verknüpfung der Daten mit der E-Mail-Adresse vorgenommen hat.[23]

In jedem Fall verfügt „Facebook" also zumindest temporär über personenbezogene Daten von Nicht-Mitgliedern. Nach einer Studie der Universität Heidelberg aus dem Jahr 2011[24] ist „Facebook" damit in der Lage, auch über Nicht-Mitglieder verlässliche Vorhersagen z.B. über

---

[21] Facebook Site Governance vom 15.11.2013, VI. Was du sonst noch wissen solltest, Freundefinder/Einladungen

[22] Der IT-Rechtsberater, 6/12, Seite133 ff.

[23] Bayerisches Landesamt für Verfassungsschutz: „Soziale Netzwerke und ihre Auswirkung auf die Unternehmenssicherheit" Studie mit der Hochschule Augsburg 2012, Seite 22

[24] One Plus One Makes Three (for Social Networks), Heidelberg Collaboratory for Image Processing (HCI) 2011

Musikgeschmack, Einkaufsverhalten etc. zu treffen.[25] „Facebook“ macht in seinen Datenverwendungsrichtlinien keine Angaben, ob und wie es die hochgeladenen Daten von Nicht-Mitgliedern verwendet.

1.5 „Facebook-timeline“ (Chronik)

Zum Jahreswechsel 2012/2013 hat „Facebook“ alle Nutzerprofile, auch die derjenigen, die Widerspruch eingelegt hatten, auf die „Chronik“ umgestellt. Eine Deaktivierung dieser Funktion ist nicht möglich; die „Chronik“ ist seither einheitliches „Pflichtprofil“ für alle User.[26]

„Facebook“ bewirbt die Chronik als Tagebuch, das ohne große Arbeit viele Bereiche des Alltags übersichtlich aufbereitet: „Timeline (Chronik) ist die Geschichte Eures Lebens. Sie lässt Euch auf neue Art ausdrücken, wer Ihr seid“,[27] so der „Facebook“-Gründer Mark Zuckerberg bei einer Präsentation des neuen Nutzerprofils im Sommer 2011. Darunter versteht „Facebook“, dass der Nutzer seine Chronik um Informationen aus der „prä-Facebook“-Ära“ ergänzen soll, indem er Inhalte (Texte, Fotos, Videos) entsprechend rückdatiert einträgt.[28] Natürlich sind auch Postings u.a. von Freunden in die Chronik rückdatiert möglich und erwünscht.

Mit der Chronik verbunden ist ein völlig neues Layout der Profilansicht. *Allerdings darf diese schönere und übersichtlichere Darstellung nicht über die damit verbundenen Risiken hinwegtäuschen. Durch die vollständige chronologische Auflistung aller jemals hinterlassenen Informationen, Bilder oder Kommentare können nicht nur peinliche „Jugendsünden“ ans Tageslicht kommen, die dem aktuellen Privat- oder Berufsleben nicht zuträglich sind. Speziell aus datenschutzrechtlicher Sicht ist vor allem bedenklich, dass die Möglichkeit, Daten und Fakten zu recherchieren, zu sammeln und zu verknüpfen, wesentlich vereinfacht wurde – was im Hinblick auf unerwünschte Besucher unangenehme Folgen haben kann…. Um sich trotz „timeline (Chronik)“ so weit wie möglich abzusichern, sollten alle jemals eingestellten Inhalte einzeln aufgerufen, auf ihre Schutzwürdigkeit überprüft und im Zweifelsfall gelöscht werden.* [29]Für Nutzer der Internet-Browser Modzilla Firefox und Goggle-Chrome empfiehlt sich eine Browser Erweiterung, die am Center for Advanced Security Research Darmstadt (CASED) in Zusammenarbeit mit der TU Darmstadt entwickelt wurde. Dieses Erweiterungstool hilft den Nutzern, ihre Privatsphäre-Einstellungen nach ihren Bedürfnissen einzurichten und zu verwalten. Mit einer einfachen „Ampelfunktion“ sieht der Nutzer auf einen Blick, welche seiner Einstellungen privat oder öffentlich sichtbar sind.[30]
Auch damit ist allerdings letztlich nicht garantiert, dass unerwünschte Inhalte nicht doch wieder in die Chronik gelangen. „Postet“ nämlich ein Freund einen gelöschten Inhalt wieder zurück, so bleibt dieser, vorerst jedenfalls, wieder in der eigenen Chronik.

---

[25] Konrad Lischka auf „Spiegel-online“ vom 10.05.2012

[26] Bayerisches Landesamt für Verfassungsschutz a.a.O., Seite 20

[27] Holger Bleich in: „Des Nutzers neue Kleider“, www.ct.de/1122098

[28] Holger Bleich a.a.O.

[29] Bayerisches Landesamt für Verfassungsschutz: „Soziale Netzwerke und ihre Auswirkung auf die Unternehmenssicherheit“ Studie mit der Hochschule Augsburg 2012, Seite 20

[30] http://www.daniel-puscher.de/fpw/

Nach dem Willen von „Facebook" ergänzt der Nutzer seine Chronik (Timeline) nicht mehr nur selbst. Apps sollen die Arbeit übernehmen: Sie posten Status und Handlungen ohne sein Zutun. Über das jüngst aufgebohrte Open-Graph-Protokoll erfährt „Facebook", was der Nutzer außerhalb so treibt und postet automatisch Status-Updates in die Timeline. Gezeigt hat Zuckerberg, wie die App des Musikdienstes Spotify die gehörten Titel in der Timeline veröffentlicht, oder wie eine Rezepte-App weitergibt, welches Mahl der „Facebook"-Nutzer gerade zubereitet. Denkbar wäre aber auch, dass Freunde in Echtzeit erfahren, welches E-Book gerade gekauft oder welcher Drink momentan in der Bar geschlürft wird. [31]

Besitzt der Nutzer ein Handy mit GPS, über das er auch mobil auf „Facebook" zugreift, wird neben den Status-updates der Standort des Nutzers übertragen[32]. „Facebook" ist damit in der Lage, von seinen Nutzern neben den Persönlichkeitsprofilen (wobei „Facebook" beteuert, keine Profile zu erstellen) auch vollständige und aktuelle Bewegungsprofile zu erstellen und auch diese Daten seinen Werbekunden zu verkaufen. So wäre es z.B. für die Kaffeehauskette „Starbucks" sicher hochinteressant zu erfahren, wie viele Personen ihrer werberelevanten Zielgruppe (die 15 bis 30-jährigen) sich aktuell auf welchen Wegen befinden. Damit könnte „Starbucks" seine Standortstrategie maximal optimieren.

[31] Holger Bleich a.a.O.

[32] Facebook Site Governance vom 15.11.2013, I. Sonstige Informationen, die wir über dich erhalten

2. Urheberrecht

2.1. „Recht am eigenen Bild", „Facebook-Gesichtserkennung"

Nach § 22 Kunsturheberrechtsgesetz „dürfen Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden." Zentral sind die beiden Begriffe „verbreiten" und „öffentlich zur Schau stellen". Entscheidend ist: Wird das Bild einem größeren Personenkreis bekannt? Das Einstellen auf eine „Facebook-Fanpage" (z.B. eines Bistums) *ist danach ohne Einwilligung nicht erlaubt, weil Fanpages auf „Facebook" – anders als persönliche Profile – immer öffentlich aufrufbar sind, z. B. auch durch Suchmaschinen wie Google oder Bing.*[33]
Gleiches gilt natürlich auch für private „Facebook-Konten" oder auch nur solche für Veranstaltungszwecke, wenn dort die Konteneinstellungen auf „öffentlich" belassen werden.

Dies stellt die Abteilungen/Dienststellen für Öffentlichkeitsarbeit der Bistümer vor Herausforderungen. Eine „Facebook-Fanpage" lebt von ihrer Aktualität. Muss vor Veröffentlichung eines Photos erst das schriftliche Einverständnis der Betroffenen eingeholt werden, *„dann können wir unsere Aktivitäten auf „Facebook" ja gleich ganz einstellen"*, so ein Öffentlichkeitsverantwortlicher erst jüngst.

Problematisch war in diesem Zusammenhang im Besonderen die Funktion der automatisierten Gesichtserkennung. Ab Mitte des Jahres 2011 nahm „Facebook" seinen Nutzern die „Arbeit", Personen auf Bildern zu identifizieren, ab. Bis dahin musste der Nutzer „mühsam" die Namen einzelner Personen auf hochgeladenen Fotos, z.B. von einer Feier, miteinander verlinken, indem er die Namen in der Kommentarzeile zu einem Bild eingab und speicherte. Seit Mitte 2011 *„versucht das System* (mit überraschender Genauigkeit!), *mittels einer Software zu erraten, wer auf einem hochgeladenen Foto zu sehen ist. Wird ein Bild ins Netz gestellt und ein Freund darauf erkannt, wird dem Nutzer vorgeschlagen, diesen zu markieren. Damit fällt die „lästige Pflicht" weg, wie es im „Facebook"-Blog heißt, eine Person dutzende Male auf jedem Foto einzeln zu markieren. …. Anstatt den Namen für jedes Foto erneut einzutippen, müsse der Nutzer die Einstellung nur einmal speichern und die Person sei auf allen Bildern eines Albums markiert. „Facebook" versieht die Bilder also nicht selbst mit Markierungen, sondern fordert die Freunde des Abgebildeten dazu auf. Dennoch dürfte die Bereitschaft der Mitglieder, vom System vormarkierte Bilder freizuschalten, größer sein, als wenn man jeden Freund manuell markieren muss. Das System erlaubt es wie gehabt, einmal vergebene Markierungen mit einem Klick zu entfernen. Wer will, dass ein Foto, auf dem er zu sehen ist, vollständig entfernt wird, muss das aber mit dem Nutzer klären, der es eingestellt hat. Löschen kann man bei „Facebook" nur Fotos, die man selbst hochgeladen hat. Wer nicht auf Fotos erkannt werden möchte, muss sich (wie bei „Facebook" üblich) durch die Privatsphäre-Einstellungen wühlen, um die Funktion inaktiv zu setzen. …. „Facebook" hat seine Nutzer bei der Einführung der Gesichtserkennung weder gefragt noch informiert, sondern sie kommentarlos in die Privatsphäre-Einstellungen integriert.*[34]

[33] #PB21 WEB2.0 in der politischen Bildung, Webschau Sept. 2011
[34] FAZ – online „Gesucht, erkannt, verlinkt" vom 08.06.2011

Millionen von Nutzern, wenigsten diejenigen, deren Profil „öffentlich“ ist, verletzten damit wissentlich oder unwissentlich täglich das „Recht am eigenen Bild“, und das auch noch weitestgehend automatisiert. Nach massiven Protesten von Datenschützern hat „Facebook“ diese Funktion für Europa im September 2012 wieder (vorläufig) deaktiviert.[35]

2.2 Veröffentlichen fremder Inhalte, „Facebook-Fanpages“

Vielfach wird schlicht übersehen, dass für „Facebook-Fanpages“ (und auch für private Konten, vor allem (aber nicht nur) wenn das Profil auf „öffentlich“ belassen wird), die normalen Regeln des Internetrechtes, des allgemeinen Medienrechtes wie auch des Urheberrechtes gelten. Dass die User hier nachlässig bzw. unwissend sind, hat mittlerweile auch die „Abmahnindustrie“ mitbekommen. *So wurde eine Kölner Kanzlei mit einer Abmahnung beauftragt, die die Veröffentlichung eines Fotos auf einer „Facebook-Pinwand“ unterbinden und mit einer Geldstrafe belegen sollte. Das Perfide dabei war, dass das Bild nicht durch den abgemahnten Seitenbesitzer, sondern durch einen „Freund“ gepostet wurde – ob dieser nun Urheber des Bildes war oder nicht, ist dabei nicht immer klar zu erkennen. Sie (der Seitenbesitzer) sind dennoch für die veröffentlichten Inhalte als „Zustandsstörer“ haftbar, egal, ob Sie oder Ihre Freunde sie posten.*[36]

Besondere Vorsicht ist geboten, wenn Texte (z.B. Zeitungsartikel), Musikstücke, Bilder, Videos, Zeichnungen etc. gepostet werden sollen, an denen noch ein Urheberrecht besteht. Hier ist in jedem Fall die vorherige schriftliche Zustimmung des Urhebers einzuholen. Allenfalls Kurzzitate oder Verlinkungen ohne Text- und/oder Bildvorschau können urheberrechtlich unbedenklich sein. Schon die Übernahme zusammenfassender Kurzberichte des Inhalts eines Artikels, Kommentare oder geänderte Darstellungen von Fotos (z.B. Fotomontagen, Verfremdungen) oder eines sonstigen Werkes, die ein Dritter legal oder illegal erstellt hat, sind ohne Zustimmung des Autors des neuen Werkes oder bei illegalen Darstellungen des Autors des Ursprungswerkes auf solchen Postings nicht erlaubt. Dies gilt auch, wenn z.B. der gepostete Zeitungsartikel ausschließlich über eine pfarrliche Aktivität berichtet, da Urheber des Artikels dennoch der jeweilige Redakteur ist.[37] Rein urheberrechtlich besteht im Übrigen kein Unterschied, ob ein Werk online, also lediglich in elektronischer Form, oder physikalisch geschaffen wurde. Nach einem Urteil des Landgerichtes Köln *kann man sich grundsätzlich nicht darauf berufen, dass ein bestimmtes Foto im Internet vorhanden und dessen Nutzung daher von der mutmaßlichen Einwilligung des Abgebildeten gedeckt ist.* [38]

Wie schon dargestellt, das allgemeine Internet- und Medienrecht gilt auch für den Betrieb von „Facebook-Fanpages“ (und nach Ansicht mancher Fachanwälte auch für private Konten, vor allem (aber nicht nur), wenn das Profil auf „öffentlich“ belassen wird. Demnach sind diese mit einem eigenen Impressum nach dem Telemediengesetz zu versehen und müssen die

[35] Fraunhofer SIT Technical Reports SIT-TR-2013-02 „soziale Netzwerke bewusst nutzen“, 2.5.1 Tagging von Bildern in Facebook, 08.2013

[36] „Schuldlose Abmahnungen bei Facebook, 4/2012 www.pcpraxis.de

[37] http://www.kerstin-hoffmann.de/pr-doktor/2010/11/23/

[38] LG Köln, Urt. vom 17.06.2009, Az. 28 O 662/08

Möglichkeit für Gegendarstellungen eröffnen.[39] Der bloße textliche Hinweis oder ein Link auf das Impressum z.B. der Bistums- oder Pfarreihomepage oder eine Verlinkung mit diesem reicht nicht aus[40].

[39] OLG Bremen, Urt. vom 14.01.2011, Az. 2O115/10

[40] OLG Düsseldorf, Urt. vom 18.12.2007, Az. I 20 U17/07

3. „Unternehmenssicherheit“

Soziale Netzwerke sind speziell für das Ansehen von Unternehmen eine Herausforderung und dürfen in ihrer Bedeutung nicht unterschätzt oder gar ignoriert werden. Nicht nur, ob oder wie sich ein Unternehmen in sozialen Netzwerken darstellt, sondern vor allem, welche Informationen andere über das Unternehmen einstellen, ist von elementarer Bedeutung. Durch die enge Vernetzung von Kontakten in einem sozialen Netzwerk werden scheinbar unwichtige Nachrichten bereits durch die einfache Statusmeldung eines Benutzers schnell verbreitet. So kann bereits ein einziger negativer Beitrag das Ansehen eines Unternehmens nachhaltig schädigen. Es muss auch davon ausgegangen werden, dass jede noch so unwichtige Kleinigkeit an die Öffentlichkeit getragen werden kann.[41]

„Facebook-Fanpages“ von Unternehmen als Werkzeug des Marketings zur positiven Präsentation in der Öffentlichkeit sind mit teils erheblichen Risiken behaftet. Diese reichen von „harmlosen“ Spam- oder Fake-Postings bis zu massiven Angriffen mit Viren und Malware. Dessen müssen sich auch kirchliche Nutzer sozialer Netzwerke, seien es die Bistümer und die Pfarr-/Kirchengemeinden, aber auch die kirchlichen Mitarbeiterinnen und Mitarbeiter selbst bewusst sein.

Häufig geht die Gefahr dabei nicht von den sozialen Netzwerken selbst aus, sondern von Werbeeinblendungen oder Anwendungen von Drittanbietern, die in diese Seiten integriert sind und Schwachstellen des jeweiligen Browsers oder Systems ausnutzen. Ein stets aktueller Antivirenschutz sowie eine aktuelle Browsersoftware ist daher für jeden Nutzer ein Muss.
Regelmäßig sollte über News-Seiten wie www.heise.de nach bekannten und insbesondere offenen Sicherheitslücken in Social-Networking-Portalen Ausschau gehalten werden. Neue Sicherheitsprobleme können an Mitarbeiter über Mailverteiler gemeldet werden, damit sich diese neuer Risiken bewusst werden. Ein Blockieren entsprechender Webseiten im Unternehmen durch die IT-Abteilung schafft nur bedingt Abhilfe, da Mitarbeiter auch von zuhause aus soziale Netzwerke nutzen. Wirklichen Schutz bieten vor allen Dingen Awareness-Maßnahmen, wie sie in der Studie „Soziale Netzwerke und ihre Auswirkung auf die Unternehmenssicherheit“ des Bayer. Landesamtes für Verfassungsschutz mit der Hochschule Augsburg 2012 ausführlich dargestellt werden. [42]

[41] Bayerisches Landesamt für Verfassungsschutz: „Soziale Netzwerke und ihre Auswirkung auf die Unternehmenssicherheit“ Studie mit der Hochschule Augsburg 2012, Seite 40

[42] Bayerisches Landesamt für Verfassungsschutz a.a.O., Seite 52 ff.

4. Empfehlungen:

(entnommen der Studie „Soziale Netzwerke und ihre Auswirkung auf die Unternehmenssicherheit“ des Bayer. Landesamtes für Verfassungsschutz mit der Hochschule Augsburg 2012, Seite 10 ff.)

Wegen der teils erheblichen Risiken und datenschutz- wie urheberrechtlichen Problemstellungen könnte eine Empfehlung eigentlich nur lauten: „Hände weg von sozialen Netzwerken.“ Da dies allerdings wegen des hohen Verbreitungsgrades sozialer Netzwerke auch bei kirchlichen Nutzern nicht (mehr) möglich erscheint, lautet die zentrale Empfehlung, soziale Netzwerke nicht nur von administrativer Seite zu blocken, sondern das Bewusstsein sämtlicher Mitarbeiter (inkl. Führungspersonal) für die Gefahren von sozialen Netzwerken – ggf. auch mit externer Hilfe – zu wecken und in geeigneten Schulungsmaßnahmen den richtigen Umgang zu vermitteln.

4.1. Empfehlungen für die Bistümer und die Pfarr-/Kirchengemeinden:

1. Keine schützenswerten Informationen publizieren. Es sollte immer das Prinzip gelten: Geheimes bleibt geheim und Internes bleibt intern. Sie sollten sich also die Frage stellen: Wissen alle Mitarbeiter, welche Informationen offen, vertraulich oder streng vertraulich sind?

2. Zurückhaltung mit offensiven persönlichen Meinungen. Wie das Beispiel der Daimler-Mitarbeiter im Zusammenhang mit Stuttgart 21 zeigt, können unbedachte Äußerungen über die eigene Firma sehr hohe Wellen schlagen. So wurde in einer „Facebook“-Gruppe der Vorstandsvorsitzende der Daimler AG als „Spitze des Lügenpacks“ beschimpft.

3. Verwenden Sie auf keinen Fall das Firmenpasswort für Ihre Zugänge bei einem sozialen Netzwerk. Diese einfache aber effektive Empfehlung wird nach wie vor zu selten umgesetzt, weil es schlicht bequemer ist, immer das gleiche Passwort zu nutzen. Genau dieser Umstand war ein riesiges Einfallstor für Angreifer in den großen, bekannt gewordenen Sicherheitsvorfällen der vergangenen Monate und Jahre.

4. Erarbeiten Sie eine eigene Position bzw. Strategie zum Thema „Soziale Medien“ – angepasst an die individuellen Gegebenheiten in Ihrem Unternehmen – und fixieren Sie diese schriftlich in einer sog. „Social Media Guideline“. Um den Aufwand gering zu halten, können Sie sich Anregungen bei der BITKOM] oder in der Policy Database von „Social Media Governance“ holen.

4.2 Empfehlungen für die Mitarbeiter/-innen

1. Vertrauen Sie nicht jeder Anfrage oder Nachricht blind. Oftmals bestätigt man zu schnell eine Freundschaftsanfrage. Dies kann zur Folge haben, dass anschließend diese (ungewollten) „Freunde“ auf wichtige Informationen zugreifen können.

2. Das gleiche gilt für Nachrichten mit ungewöhnlichen Inhalten. Es gibt eine Reihe von Angriffen, die deshalb erfolgreich sind, weil man das Opfer dazu bringt einem Link zu folgen. Gerade bei Twitter ist es üblich, dass Kurzlinks verwendet werden und somit die eigentliche Zieladresse nicht bekannt ist.

3. Veröffentlichen Sie keine allzu privaten oder gar intimen Details oder Bilder – nicht nur um hier keine Angriffsfläche für Social Engineering, Erpressung oder Diffamierung zu bieten. Auch Personalchefs recherchieren heutzutage standardmäßig im Internet, bevor sie jemanden einstellen.

4. Überprüfen Sie Ihre „Privatsphäre“-Einstellungen und regulieren Sie diese entsprechend Ihrer tatsächlichen Nähe zu dem Personenkreis, der Ihre privaten Postings wirklich lesen oder kennen soll.

5. Wer Karrierenetzwerke wie XING als Jobbörse nutzt, sollte darauf achten, sein Profil möglichst aktuell zu halten und so einzustellen, dass sein Name von Suchmaschinen gefunden wird, um für suchende Unternehmen interessant zu bleiben oder zu werden.

6. Um zu überprüfen, was bereits offen über Sie im Netz recherchierbar ist, sollten Sie regelmäßig Ihren eigenen Namen in den verschiedenen Suchmaschinen checken. Zusätzlich kann ein „Google Alert“ mit Ihrem Namen dafür sorgen, dass Sie immer sofort informiert werden, wenn online etwas Neues über Sie auftaucht.

7. Halten Sie sich über Neuerungen oder Änderungen Ihres verwendeten sozialen Netzwerks auf dem Laufenden. Sobald Sie durch eine Mail des Betreibers z.B. über eine wichtige Datenschutzänderung informiert worden sind, gilt diese für Sie als verbindlich.

8. Ein Punkt, der viele aufgrund des Aufwandes abschreckt, aber wichtig ist: Machen Sie sich bewusst, welche Rechte Ihrer veröffentlichten Inhalte (Video, Bilder, Texte) an den Betreiber der Plattform übergehen. Mehr dazu finden Sie in den Beschreibungen der einzelnen Netzwerke.

9. Grundsätzlich gilt: Verhalten Sie sich in sozialen Netzwerken den Mitgliedern gegenüber so, wie Sie es auch im realen Leben tun würden.

5. Muster für „social-media-guidelines“

(nach: Erzbistum Köln, Stabsabteilung Medien, Petra Dierkes)

Richtlinien zur Nutzung sozialer Medien für Mitarbeiterinnen und Mitarbeiter des (Erz-)Bischöflichen Generalvikariats in ….

Vorbemerkung

Folgende Richtlinien richten sich an alle Mitarbeiterinnen und Mitarbeiter des (Erz-)Bistums …. sowie seiner Einrichtungen, die sich dienstlich mit Social Media angeboten befassen. Sie sollen Ihnen helfen, sich privat und auch dienstlich verantwortungsvoll und sicher in sozialen Netzwerken zu bewegen. Als Soziale Medien werden alle Medien-Plattformen verstanden, die über digitale Kanäle genutzt werden. Sie dienen der Information und Kommunikation und bieten darüber hinaus die Chance, eigene Inhalte zu verbreiten.

Handeln Sie verantwortlich

Als Katholikinnen und Katholiken sind wir zum Dialog mit anderen Menschen und Gruppen aufgerufen und herausgefordert. Soziale Medien und Netzwerke unterstützen dieses Miteinander. Im Bereich der sozialen Medien bewegen sich die Mitarbeitenden des …, wie sonst auch, im Spannungsfeld zwischen dem Grundrecht auf Meinungsfreiheit und der Pflicht zur Loyalität gegenüber dem Arbeitgeber. Wenn Sie in Ihren Profilen als Mitarbeiterin oder Mitarbeiter des EGV in Erscheinung treten, verschwimmen die Grenzen zwischen Berufs- und Privatleben.

Es ist zu unterscheiden zwischen offiziellen Stellungnahmen als Mitarbeiterin oder Mitarbeiter des … und Äußerungen als Privatperson. Auf privater Ebene entscheiden Sie selbst, ob Sie in sozialen Netzwerken angeben, dass Sie im Generalvikariat des (Erz-)Bistums …. arbeiten, bei dienstlicher Nutzung muss dies bei der Kommunikation in sozialen Medien deutlich bei der Profileinstellung angegeben werden. Nach Bedarf werden Schulungen und Informationen in diesem Bereich für alle Mitarbeitenden angeboten.

Seien Sie erkennbar

Transparenz bei der dienstlichen Nutzung stellen Sie her, wenn Sie Ihren Beitrag in der Ich-Form schreiben, Ihre Funktion innerhalb des … angeben, Ihren Klarnamen und kein Pseudonym verwenden. Weisen Sie darauf hin, wenn Sie bewusst als Privatperson eine Meinung äußern. Der Unterschied sollte für Dritte deutlich werden, da sonst die Gefahr der Verwechslung von dienstlichen und privaten Äußerungen besteht.

Seien Sie freundlich

Verwenden Sie einen freundlichen und wertschätzenden Sprachstil. Hören Sie zu, antworten Sie auf Fragen und mischen Sie sich ein, wo Sie etwas sagen sollten. Beleidigungen und abwertende Kommentare aufgrund von Geschlecht, Religion oder ethnischer Herkunft sind

tabu, ebenso kirchenfeindliches Verhalten oder Äußerungen, die sich gegen die katholische Glaubens- und Sittenlehre wenden.

Seien Sie respektvoll

Soziale Netzwerke sind ein öffentlicher Raum. Was Sie veröffentlichen, ist potentiell für alle Menschen sichtbar. Aussagen zurückzunehmen ist schwierig bis unmöglich; selbst wenn Sie den Inhalt für den allgemeinen Zugriff gesperrt haben, kann ein „Freund" diesen (un)absichtlich an andere weiterleiten. Soziale Netzwerke sind für vertrauliche, schützenswerte Kommunikationen, auch wenn sie in nichtöffentlichen Teilen solcher Netzwerke stattfindet (Chats etc.), nicht geeignet. Sie können deshalb z.B. die Kommunikation über gesicherte Email-Adressen nicht ersetzen.

Seien Sie diskret und achten Sie die Gesetzte

Bestimmte Informationen dürfen aus dem beruflichen Kontext auch laut den Datenschutzregelungen des Hauses nicht veröffentlicht werden. Dazu gehören vor allem vertrauliche Informationen aus dem … oder berufliche Daten zu Kolleginnen, Kollegen und Externen. Seien Sie aber auch mit privaten Informationen über andere Personen zurückhaltend. Denken Sie daran: Wenn Sie Texte, Fotos, Musikstücke, Filme oder auch Markenlogos in Ihre Seiten einbinden wollen, ist zuvor die Erlaubnis von Autorinnen und Autoren, bzw. von den Urhebern einzuholen.

Seien Sie dabei

Eine verantwortungsvolle Nutzung Ihres Auftritts bei sozialen Medien während der Arbeitszeit ist möglich. Klären Sie aber zuvor mit Ihren Vorgesetzten, in welchem zeitlichen Umfang Sie für berufliche Zwecke Kontakte knüpfen, sich Wissen aneignen, Netzwerke aufbauen und somit für das … tätig werden können.

Wenn Sie Fragen haben, wenden Sie sich bitte an:

Index: