AC Tischendorf Rechtsanwälte

ACT Knowledge Breakfast

„Social Media am Arbeitsplatz“ – Die Umsetzung

Stand 15.06.2012

www.ac-tischendorf.com

Inhaltsverzeichnis

Allgemeine Tipps zur Einführung von Social Media

Social Media-Nutzung am Arbeitsplatz -Erlaubt?

- Gilt eine Privatnutzungserlaubnis für den dienstlichen PC auch für iPhone, iPad und Co.?
  - Strittig. Meines Erachtens nein, weil
    - Gesonderte Verträge mit Dienstanbietern erforderlich sind
    - Zusätzliche Kosten entstehen können
    - Arbeitgeber weniger Einfluss auf tatsächliche Nutzung der mobilen Geräte haben und erhöhte Missbrauchsgefahr (z.B. durch Herunterladen bestimmter Applikationen) besteht.
    - Übliche Programme zum Schutz vertraulicher Daten bei Verlust/ Diebstahl sogar strafrechtlich relevant, § 303a StGB

Empfehlung

1. Konkrete Festlegung, welche Dienste in welchem Umfang privat genutzt werden dürfen.
2. Schriftliche Einwilligung bzgl. Kontrolle, Virenschutz, „remote erase“ einholen

Social Media-Nutzung am Arbeitsplatz -Erlaubt?

- Anspruch auf Privatnutzung aufgrund betrieblicher Übung?
  - Tatsächliche Privatnutzung über einen längeren Zeitraum (Achtung: „Scheinverbot“)
  - Erkennbare Duldung, das heißt:
    - Kenntnis von der Privatnutzung und deren Umfang
    - Ein nach Außen tretendes Verhalten des Arbeitgebers, aus dem sich ergibt, er akzeptiere die Privatnutzung auch für die Zukunft.

    Erkennbare Duldung, das heißt:
  - Keine anderweitigen Rechtsgrundlagen
  - Keine wirksamen Freiwilligkeits- und/ oder Schriftformklauseln in den Arbeitsverträgen

- Rechtsfolge
  - Rechtsanspruch auf Privatnutzung im bisherigen Umfang

Social Media-Nutzung am Arbeitsplatz – „Schatten-IT“ im Unternehmen?

- Risiken der Nutzung privater Smartphones & Co.
  - Vertrauliche Daten werden auf nicht von der IT-Sicherheit geprüfte private Geräte gespielt.
  - Ferngesteuerte Löschung ist bei Verlust/ Diebstahl nicht möglich.
  - Nicht ausreichend geschützte Privatgeräte im ungeschützten WLAN-Netz

Empfehlung

1. Konkrete Weisungen und Richtlinien (bzw. Betriebsvereinbarungen), dass private Geräte nicht genutzt oder nur bestimmte, von der IT-Abteilung genehmigte und in das Sicherheitssystem eingebundene Geräte eingesetzt werden dürfen.
2. Untersagung der Nutzung ungesicherter Netze
3. Regelung des konkreten Nutzungsumfangs privater Geräte am Arbeitsplatz

Social Media-Nutzung am Arbeitsplatz

- Weisungen des Arbeitgebers hinsichtlich der Darstellungsweise seiner Arbeitnehmer in Berufsnetzwerken, z.B. Xing?
  - Grundsatz: Keine Weisungsrechte, Nutzungsverbote bei privater Nutzung (Weihnachtsfeier?)
  - Ausnahme:
    - Nutzung für geschäftliche Zwecke, z.B. Kundenakquise
    - Entfernung unrichtiger Darstellungen, z.B. Nennung eines falschen Jobtitels
    - Löschung rufschädigender Arbeitnehmerportale, z.B. abschätzige Kommentare

Empfehlung

1. Einrichtung von Unternehmensauftritten
2. Maßgeschneiderter Auftritt im Netzwerk auch zur Wahrung der Corporate Identity
3. Nutzung für Recruiting-Zwecke
4. Corporate Identity definieren (wie will ich nach Außen auftreten?)

Implementierung von Nutzungs ordnungen

Verbot oder Anweisung – Rechts grundlagen

- Die private Nutzung von Social Media am Arbeitsplatz kann geregelt werden durch:
  - **Arbeitsvertrag** (Einführung in bestehenden Arbeitsverhältnissen nur einvernehmlich; spätere Anpassung aufwendig)
  - **Betriebliche Übung?** (keine negativen Veränderungen)
  - **Betriebsvereinbarung** (umfassendere Regelungen sinnvoll rechtlich möglich; Verhandlungen mit dem BR generalstabsmäßig planen und angehen)
    - ➢ Regierungsentwurf 08/2010: Klarstellende Regelung in § 4 Abs. 1 S. 2 BDSG: „Andere Rechtsvorschriften im Sinne des Gesetzes sind auch Betriebs- und Dienstvereinbarungen.“
  - **Einseitige Vorgabe durch den Arbeitgeber/Richtlinie** (Inbezugnahme/ Empfangsbekenntnisse)

TIPP

Regelungen einschließlich internettauglicher mobiler Geräte, z.B. iPhone

Verbot oder Anweisung- Nutzen

- Social Media Nutzungsordnungen
  - ermöglichen es, den Umfang des erlaubten Gebrauchs von Social Media konkret zu definieren,
  - sensibilisieren und fördern einen verantwortungsvollen Umgang der Mitarbeiter mit Social Media,
  - dienen einer Nutzung entsprechend der Unternehmenskultur, und
  - erleichtern individualrechtliche Sanktionen, sofern es zu Verstößen kommt.

Verbot oder Anweisung- Hinweise

- Das sollten Sie beachten:
  - Differenzierung Sie zwischen unverbindlichen Handlungsempfehlungen und verbindlichen Vorgaben:
    - bei privater Nutzung des Arbeitnehmers außerhalb des Arbeitsplatzes sind allenfalls unverbindliche Handlungsempfehlungen möglich
    - Klarstellende Differenzierung zwischen zulässiger Meinungsäußerung und unzulässiger Schmähkritik sinnvoll
    - Hinweis auf mögliche Sanktionen
  - Treffen Sie eine klare Aussage zum erlaubten Nutzungsumfang
  - Fordern Sie den Arbeitnehmer auf, Betriebsgeheimnisse zu wahren

Verbot oder Anweisung- Hinweise

- Fordern Sie den Arbeitnehmer auf, gesetzliche Vorgaben einzuhalten:
  - Insbesondere Beachtung der Urheber-, Wettbewerbs- und Persönlichkeitsrechte sowie des Datenschutzes
  - Beispiel: Recht am eigenen Bild (Firmenfeier)
  - Beispiel: Schleichwerbung / Eigenwerbung (UWG)

- Empfehlen Sie dem Arbeitnehmer, Transparenz zu wahren und seine eigene Meinung als solche kenntlich zu machen

Überwachung der Kommunikation

- Checkliste: Betriebsvereinbarung IuK-Anlagen-Nutzung

✓	IuK-Anlagen, die vom AG zur Verfügung gestellt werden
✓	Dienstliche und/oder private Nutzung, Grenzen
✓	Konkretisierung des Umfangs der arbeitgeberseitigen Kontrolle (Bezeichnung der Art der gespeicherten Daten, Kontrollperson, Kontrollverfahren)
✓	Freiwilligkeit/ Einwilligung in Eingriff ins Fernmeldegeheimnis
✓	Maßnahmen zur Aufklärung von Missbrauchsfällen (anlassbezogen, stichproben-bezogen)
✓	Regelungen zum Vertretungsfall bei Abwesenheit
✓	Technische und organisatorische Schutzmaßnahmen (PIN, Passwörter, Virenschutz-programm)
✓	Datenschutzverpflichtung

TIPP

Koppelung der privaten Nutzungsmöglichkeit an Einwilligung!

Überwachung der Kommunikation

- Checkliste: Besonderheiten bzgl. Social-Media-Angeboten

✓	Schaffung von Problembewusstsein bei der Herausgabe vertraulicher Unternehmensinformationen in sozialen Netzwerken
✓	Verbot der Nutzung von Unternehmenslogos, etc.
✓	Verbot der Verwendung von Firmen-E-Mail-Adressen (Gefahren: Benachrichtigungen, Zugriff auf Firmen-Adressbücher)
✓	Bei mobilen Geräten (iPhone & Co.) ➢ Verbot des „Jailbreaks“ ➢ Keine Schatten-IT ➢ Nutzung von Codes-Sperren ➢ Unverzügliche Meldung bei Verlust ➢ Keine Datendienste im Ausland ➢ Keine Nutzung unsicherer Netze (WLAN im Hotel, Flughafen, etc.)

Sonderthema: Arbeitsrechtliche Einwilligung

Ausgestaltung der Einwilligung

- Ist die Einwilligung eines AN nach § 4a BDSG „freiwillig“?
  - Freiwillig → „ohne jeden Zweifel“, „ohne Zwang“
  - Grenze: Rechtsmissbrauch
  - Keine Erweiterung des Fragerechts, d.h. keine Umgehung zwingender Schutznormen durch Einholung der Einwilligung
  - Konkretheit der Einwilligung, d.h. der AN muss wissen, für welche konkrete Verwendung er die Einwilligung erteilt
  - Schriftform, drucktechnisch hervorzuheben

    „Generaleinwilligung“ mangels Konkretheit allenfalls Information nach § 4 Abs. 2 BDSG; nicht gleich-zeitig mit Arbeitsvertragsschluss

Regierungsentwurf 08/2010:

Neueinführung des § 32l BDSG: Einwilligung nur, soweit ausdrücklich durch §§ 32 ff. BDSG zugelassen.

- **Regierungsentwurf 08/2010:** 7 zugelassene Einwilligungen

Norm	Zugelassene Fälle der Einwilligung
§ 32 Absatz 6 Satz 4	Bewerbungsverfahren: Nur mit Einwilligung des Bewerbers darf der Arbeitgeber Auskünfte bei „sonstigen Dritten“ (z.B. Vor-AG) einholen.
§ 32a Abs.1 S.2 Abs.2 S.2	Ärztliche Untersuchung/Eignungstest im Bewerbungsverfahren: Nur mit Einwilligung des Bewerbers ist die ärztlichen Untersuchung oder Prüfung sowie Mitteilung des Ergebnisses an den AG zulässig.
§ 32b Absatz 3	Aufbewahrung in Bewerbungsdaten: Nur mit Einwilligung des Bewerbers zulässig.
§ 32c Absatz 3	Ärztliche Untersuchung/Eignungstest im laufenden Arbeitsverhältnis: Nur mit Einwilligung des Beschäftigten ist die ärztlichen Untersuchung oder Prüfung sowie Mitteilung des Ergebnisses an den AG zulässig.
§ 32h Absatz 1 Satz 2	Biometrische Verfahren: Ausschließlich Lichtbilder können mit Einwilligung des Beschäftigten zu anderen als Autorisierungs- und Authentifikationszwecken genutzt werden.
§ 32i Absatz 2 Satz 1	Ausschließlich dienstliche Nutzung von Telefonen: Aufzeichnung von Inhalten bedürfen der Einwilligung des Beschäftigten und den Kommunikationspartners im konkreten Einzelfall.
§ 32i Absatz 2 Satz 2	Besonderheit Callcenter: Aufzeichnung von Inhalten zulässig bei Einwilligung von Beschäftigten und Kommunikationspartner in mögliche Aufzeichnung in einem festgelegten Zeitraum.

Umsetzung einer IT Richtlinie

IT Richtlinie

Präambel

Mit dieser IT-Richtlinie sollen einheitliche Regelungen für die Nutzung von Computerarbeitsplätzen, Intranet, Internet und E-Mail (zusammen „IT-Infrastruktur“) durch die Mitarbeiter der ABC GmbH („Unternehmen“) geschaffen werden.

Ziel der Richtlinie ist es, sowohl die Sicherheit, Integrität und Funktionalität der IT-Infrastruktur und den Schutz der Geschäfts- und Betriebsgeheimnisse des Unternehmens zu gewährleisten, als auch das Persönlichkeitsrecht der Mitarbeiter und den Schutz ihrer personenbezogenen Daten sicherzustellen.

Die nachfolgenden Regelungen sind erforderlich, um die gesetzlichen Vorgaben im Hinblick auf die Aufbewahrung von Geschäftsunterlagen, den Schutz personenbezogener Daten und das Fernmeldegeheimnis einzuhalten und die Compliance-Anforderungen des Unternehmens zu erfüllen

Festlegung des Zwecks der Richtlinie und Begründung der Notwendigkeit

Pflicht zur ordnungsgemäßen Unternehmensführung beinhaltet interne Organisationsstruktur, um die Rechtmäßigkeit und Effizienz des Handelns der Gesellschaft gewährleistet

IT Richtlinie

1. Grundsätze der Nutzung

Das Unternehmen stellt im erforderlichen Umfang IT-Infrastruktur zur Erbringung der vertraglichen Arbeitsleistung zur Verfügung. Die Nutzung der betrieblichen E-Mail-Systeme ist ausschließlich der dienstlichen Nutzung vorbehalten. Eine private Nutzung ist nicht gestattet. [….].

Grundsatzentscheidung, ob die IT ausschließlich dienstlich oder ganz oder teilweise privat genutzt werden darf

2. Allgemeine Regeln der Nutzung

2.1 Das Unternehmen stellt nach eigenem Ermessen und im erforderlichen Umfang Computerarbeitsplätze zur Arbeitsleistung zur Verfügung. [….].

2.2 Der Mitarbeiter hat keinen Rechtsanspruch auf Überlassung eines Computerarbeitsplatzes mit den vorstehend beschriebenen Zugangsmöglichkeiten.

Zweckbestimmung

Freiwilligkeit der Bereitstellung wirkt betrieblicher Übung entgegen

IT Richtlinie

2.3 *[Zugangskennung und Passwort]*

2.4 Jeder Mitarbeiter ist verpflichtet, seinen Computerarbeitsplatz vor unberechtigtem Zugriff zu schützen. Ein Zugang in das System ist nur den berechtigten Personen und nur über ihr eigenes Passwort erlaubt. Passwörter sind geheim zu halten und bei jedem Verlassen des Arbeitsplatzes ist der Computerarbeitsplatz zu sperren.

2.5 Jeder Computerarbeitsplatz darf nur mit der vom Unternehmen zur Verfügung gestellten Hard- und Software ausgestattet sein. Erweiterungen und Ergänzungen sind zustimmungspflichtig. [….].

Datensicherheit und Schutz der IT

An die gesonderte Verpflichtung der Admin denken! Protokollierung des Zugriffs auch zum Schutz der Mitarbeiter und des Admins

Zweck: Datensicherheit und Schutz der IT; gegebenenfalls zusätzliche technische Maßnahmen einrichten

3. Nutzung von Internet und Intranet

3.1 Das Unternehmen verfügt über ein betriebsinternes Intranet und Zugang zum externen Internet. Das Intranet dient als interne Informationsplattform [….].

Intranet geeignet für Unternehmenskommunikation, Schulungen, Richtlinie, Handlungsanweisungen etc.

IT Richtlinie

3.2 Bei der Nutzung von Intranet und Internet sind die folgenden Maßgaben zu beachten:

(i) Das Unternehmen behält sich vor, bestimmte Internetseiten zu sperren, sofern Gefahr besteht, dass diese rechtswidrige Inhalte oder schädliche Software enthalten oder den Betriebsablauf stören.

(ii) Bei der Nutzung des Internet sind Verhaltensweisen zu vermeiden, welche die Reputation des Unternehmens oder deren Vertreter beeinträchtigen können.

(iii) Das Aufrufen oder Verbreiten von Inhalten, die gegen datenschutzrechtliche, urheberrechtliche oder sonstige gesetzliche Bestimmungen verstoßen, ist untersagt.

(iv) [….]

Vorbehalt der Einschränkung ← betriebliche Übung

Z.B. negative Äußerungen im Internetz, in social media, blogs u.ä.

Wichtig für Haftungsprivilegierung des Unternehmens nach TMG

IT Richtlinie

3.2 Die private Nutzung des Internets ist erlaubt, wenn der Mitarbeiter gegenüber dem Unternehmen die als **Anlage** beigefügte (widerrufliche) Einwilligung abgibt, dass das Unternehmen von der Einhaltung datenschutz-, telekommunikations- und persönlichkeitsrechtlicher Vorschriften befreit ist. Soweit ein Mitarbeiter keine Einwilligungserklärung abgibt oder sie widerruft, ist ausschließlich die dienstliche Nutzung des Internet erlaubt.

3.3 Bei der privaten Nutzung des Internets sind folgende Regeln ergänzend zu beachten:

(i) Die private Nutzung ist ausschließlich außerhalb der Arbeitszeit erlaubt.

(ii) [….].

Einwilligungslösung

Folge: Weitergehende Kontrollrechte des Unternehmens

4. Nutzung des E-Mail-Systems

4.1 Die Nutzung des E-Mail-Zugangs ist intern wie extern zu dienstlichen Zwecken nach Maßgabe der folgenden Regelungen erlaubt:

(i) Nachrichten mit vertraulichem Inhalt dürfen per E-Mail nur verschlüsselt verschickt werden. Der Systemadministrator hat hierfür die geeignete Verschlüsselungstechnologie eingerichtet.

(ii) Bei vorübergehender Abwesenheit, z.B. wegen Urlaubs, Krankheit oder sonstiger ganztägiger Abwesenheit, hat der Mitarbeiter auf geeignete Weise sicherzustellen, dass eingehende E-Mails in Absprache mit seinem Vorgesetzten an den Vertreter weitergeleitet werden und ein Abwesenheitsassistent aktiviert wird. [….]

Rein dienstliche Nutzung

Haftung des Unternehmens, Datenschutz (insb. §42a BDSG) und Datensicherheit

Wichtig: Vorher festlegen, weil nachträglicher Zugriff rechtlich und faktisch kaum möglich

IT Richtlinie

(iii) Im Falle einer unvorhergesehenen Abwesenheit oder wenn der Mitarbeiter die Weiterleitungsfunktion oder den Abwesenheitsassistenten nicht eingestellt hat, wird der Systemadministrator in Absprache mit dem Vorgesetzten des Mitarbeiters sicherstellen, dass eingehende E-Mails an einen Vertreter weitergeleitet werden und einen Abwesenheitsassistenten aktivieren.

(iv) Eine automatische Weiterleitung an externe E-Mail-Adressen ist nicht gestattet. [….]

(v) Das Versenden einer E-Mail hat mit der Sorgfalt und im Stile eines dienstlichen Schreibens zu erfolgen. Das Unternehmen wird auch über die dienstlichen E-Mails seiner Mitarbeiter nach außen repräsentiert. Deshalb sind Verhaltensweisen, welche die Reputation des Unternehmens oder deren Vertreter beeinträchtigen können, zu vermeiden. [….]

U.a. Datensicherheit und Know-How Schutz

Wichtig für Haftungsprivilegierung des Unternehmens nach TMG

IT Richtlinie

4.2 Eine Nutzung zu privaten Zwecken ist verboten. Missbrauchsfälle können je nach Schweregrad zum Widerruf der Zugangsberechtigung und zu arbeitsrechtlichen Konsequenzen bis hin zur fristlosen Kündigung führen.

4.3 *[Firewall und Anti-SPAM-Software]*

4.4 *[Beendigung des Arbeitsverhältnisses]*

Ausschluss privater Nutzung; Ggf. Web-mail oder separates Konto

IT Richtlinie

4.5 Alle ein- und ausgehenden E-Mails mit Anhängen werden zur Einhaltung der gesetzlichen Aufbewahrungspflichten sowie zur Sicherung gegen Datenverlust automatisch gesichert und archiviert. [….].

4.6 *[Einsichtnahme durch Vorgesetzten]*

4.7 *[Lesen und Auswerten von E-Mails]*

Aufbewahrungsfristen nach HGB und AO Rechtfertigung für Datenspeicherung

Wichtig: Vorher festlegen, weil nachträglicher Zugriff rechtlich und faktisch kaum möglich

IT Richtlinie

5. Speicherung und Auswertung von Daten

5.1 Zum Schutze der Systemsicherheit und –funktionalität und vor Missbrauchsfällen speichert das Unternehmen die nachfolgenden Daten über Benutzeraktivität im Internet und der Telekommunikation („gespeicherte Daten“):

(i) [….],

(ii) [….],

(iii) [….],

(iv) [….].

Wichtig ist die konkrete Benennung der gespeicherte Datenarten, weil nur dann eine datenschutzrechtliche Einwilligung wirksam ist

IT Richtlinie

5.2 Zur stichprobenartigen Kontrolle der Einhaltung dieser IT-Richtlinie, bei dem Verdacht missbräuchlicher oder sonstiger dieser IT-Richtlinie nicht entsprechender Nutzung, sowie bei dem Verdacht einer Verletzung sonstiger arbeitsvertraglicher Pflichten durch den Mitarbeiter ist eine Auswertung der gespeicherten Daten durch den Systemadministrator zulässig. Eine Auswertung wird nicht zum Zwecke einer allgemeinen Leistungs- und Verhaltensüberprüfung des Mitarbeiters durchgeführt. [….]

5.3 *[Auswertungsergebnisse]*

5.4 *[Löschung der Daten]*

5.5 *[Zugang und Auswertung]*

Risikomanagement: Nicht nur Aufgabenverteilung im Unternehmen, sondern auch risikoreduzierende Kontrollstukturen, also Einrichtung eines Risikomanagementsystems.

IT Richtlinie

6. Rechtsfolgen bei Missbrauch und Missbrauchsverdacht

6.1 Das Unternehmen kann die Zugangsberechtigung zu Intranet, Internet und E-Mail-Kommunikation im Falle eines Missbrauchs oder eines sonstigen Verstoßes gegen diese IT-Richtlinie ganz oder teilweise widerrufen. [….]

6.2 Bei schweren Missbrauchsfällen oder schwerwiegenden Verstößen gegen diese IT-Richtlinie kann es zudem zu arbeitsrechtlichen Konsequenzen kommen [….].

6.3 Die Berechtigung zur privaten Nutzung des Internet kann bereits widerrufen werden, wenn sich objektive Verdachtsmomente für eine missbräuchliche Nutzung ergeben, oder wenn der Mitarbeiter die schriftliche Einwilligung widerruft. Der betroffene Mitarbeiter ist vorher anzuhören.

Compliance-management: Pflicht zur Errichtung organisatorischer Vorkehrungen, die die Begehung von Gesetzesverstößen durch Mitarbeiter der Gesellschaft verhindern.

Umsetzung einer Social Media Guideline

Social Media Guideline - Grundsätze

1. Definieren Sie Ziele.
2. Geheimnisse sind geheim und Interna bleiben intern.
3. Mitarbeiter müssen authentisch sein.
4. Wer veröffentlicht, übernimmt Verantwortung.
5. Interne Kritik ist erlaubt, bleibt aber intern.
6. Gehen Sie mit Fehlern offen um.
7. Schonen Sie Ihre Geschäftsbeziehungen.
8. Beachten Sie das geltende Recht.
9. Schränken Sie private Nutzung von Social Media während der Arbeitszeit ein.
10. Social Media erfordert kontinuierliches Engagement.

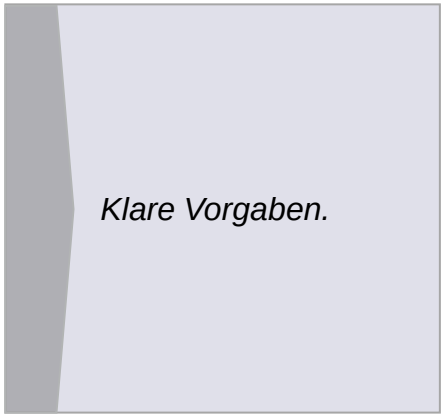
Klare Vorgaben machen.

Social Media Guideline - Grundsätze

1. Trennung von Privat und Beruflichen

   Wenn sich der Mitarbeiter ohne einen dienstlichen Auftrag in sozialen Medien zu einem Thema äußert, ist deutlich zu machen, dass der Mitarbeiter seine persönliche Meinung vertritt und nicht für das Unternehmen spricht. Es ist daher immer die Formulierung "ich" statt "wir„ zu verwenden.

2. Es ist der persönliche Beitrag, der in sozialen Medien zählt. Daher sind Beiträge mit dem Klarnamen zu versehen, um über die Identität des Verfassers Klarheit zu haben.



Social Media Guideline - Grundsätze

3. Verantwortlichkeit

3.1 Der Mitarbeiter ist für das, was er in sozialen Netzwerken tut und veröffentlicht, selbst verantwortlich. Der Mitarbeiter hat bewusst mit dieser Verantwortung in seinem eigenen Interesse und im Interesse des Arbeitgebers umzugehen.

3.2 Beiträge in sozialen Netzwerken sind öffentlich - und das unter Umständen sehr lange. Der Mitarbeiter ist sich dieser Tragweite seiner Beiträge bewusst und bewahrt auch in hitzigen Debatten einen kühlen Kopf. Der Mitarbeiter ist verpflichtet, stets sachlich zu argumentieren, niemanden zu beleidigen und respektvoll im Umgang mit Dialogpartnern zu sein. Hierbei hat sich jeder Mitarbeiter an die unternehmensweiten **Ethikrichtlinien** zu halten.

Bewusstsein schaffen.

Stellen Sie Verhaltensregeln im Rahmen von Ethikrichtlinien auf.

Social Media Guideline - Grundsätze

4. Arbeitszeit

   Die Social Media-Nutzung bringt es mit sich, dass häufig private und dienstliche Nutzung ineinander übergehen. Was die private Nutzung während der Arbeitszeit betrifft, so ist diese innerhalb des Unternehmens in der Betriebsvereinbarung zur Nutzung der Kommunikationseinrichtungen geregelt. Soweit erforderlich, hat der Mitarbeiter die Zeitkorrektur-Buchungen im Zeiterfassungssystem zu nutzen.

Vertrauensarbeitszeit oder strengere Regelungen?

Anhang – Beispiele für Social Media Richtlinien

[redacted] AG

Social Media Leitfaden

Das Internet ist aus unserer Gesellschaft nicht mehr wegzudenken. Zurzeit gewinnt vor allem die Nut-zung von Social Media Angeboten mehr und mehr an Bedeutung. Unter dem Begriff „Social Media" werden Plattformen und Netzwerke zusammengefasst, bei denen die Nutzer die Möglichkeit haben beispielsweise Fotos, Videos, aber auch Erfahrungsberichte oder Meinungen auszutauschen. Dazu zählen unter anderem Blogs, Wikipedia, YouTube, Facebook oder auch Twitter.

Die wachsende Beliebtheit von Social Media ist auch für Unternehmen von großer Bedeutung: Nutzer sprechen im Internet über Firmen, diskutieren über neue Technologien und empfehlen Produkte – oder eben nicht. Wer diese Diskussionsplattformen ignoriert, der ignoriert auch einen äußerst wirksamen Kommunikationskanal. Social Media Engagement kann helfen, Trends frühzeitig zu erkennen, auf Kritik zu reagieren oder eigene Themen anzustoßen. Und wer könnte das Unternehmen und seine Vielfalt in der Öffentlichkeit besser darstellen als die Mitarbeiter? Mit Ihrem Expertenwissen können Sie Diskussionen im Internet bereichern oder nützliche Anregungen für Ihre Arbeit finden.

Es ist daher im Interesse der [redacted] AG, Ihr Engagement im Bereich Social Media zu fördern. Allerdings stellen wir auch immer wieder fest, dass es im Umgang mit diesen Kommunikationsformen noch viele Unsicherheiten gibt. Um Sie über die Möglichkeiten und Risiken der beruflichen Nutzung zu informieren, haben wir die folgenden Hinweise zusammengestellt. Soweit es dabei nicht um gesetzlich vorgeschriebene Dinge geht, handelt es sich ausdrücklich nicht um Gebote sondern um Empfehlungen, die Ihnen beim Umgang mit Social Media helfen sollen.

Beispiel

10 Tipps zum Umgang mit Social Media

1. **Es geht immer um Konversation.** Wenn Sie Social Media nur für Einbahnstraßenkommunikation nutzen, reden Sie bald gegen eine Wand. Nur wer aktiv das Gespräch sucht, sich in Diskussionen zu Wort meldet und auf Fragen antwortet wird im Web 2.0 ernst genommen.
2. **Achten Sie auf Qualität.** Es ist einfach, im Internet schnell und viel Aufmerksamkeit zu erhalten. Langfristige, intensive und wertvolle Konversationen lassen sich aber nur mit qualitativ hochwertigen Inhalten anstoßen bzw. bereichern.
3. **Seien Sie ehrlich.** Lügen haben im Internet besonders kurze Beine. Informationen sind im Netz sofort nachprüfbar. Falschaussagen oder oft auch nur Weglassungen werden umgehend aufgedeckt und schaden Ihrer Glaubwürdigkeit.
4. **Bleiben Sie höflich.** Eine Konversation kann nur wertvoll sein, wenn sich alle Beteiligten respektvoll begegnen. Vermeiden Sie Provokationen und Beleidigungen und brechen Sie Gespräche ab, wenn der Gesprächspartner beleidigend wird.
5. **Achten Sie das Gesetz.** Veröffentlichen Sie keine verleumderischen, beleidigenden oder anderweitig rechtswidrigen Inhalte. Stellen Sie keine Inhalte ohne entsprechende Urheberverweise ins Netz und beachten Sie Copyrights. Respektieren Sie das Recht am eigenen Bild. Halten Sie unter-nehmensbezogene Informationen geheim, die sich auf den Börsenpreis von [redacted]-Wertpapieren auswirken könnten. Solange Sie Zugang zu solchen öffentlich nicht bekannten Informationen haben, dürfen Sie keinem anderen den Kauf oder Verkauf von [redacted]-Wertpapieren empfehlen oder andere Personen in sonstiger Weise dazu verleiten.
6. **Berichtigen Sie eigene Fehler.** Viele Nutzer im Web 2.0 sind schnell verärgert, verzeihen aber auch rasch. Geben Sie eigene Fehler zu und berichtigen Sie diese. Es empfiehlt sich, diese Änderungen so vorzunehmen, dass sie nachvollziehbar sind, um Missverständnisse oder Irritationen zu vermeiden.

Beispiel

7. **Seien Sie auch als Privatperson professionell**. Auch wenn Sie Social Media „nur“ privat nutzen, kann es vorkommen, dass Sie auf berufliche Kontakte stoßen oder mit Fragen aus Ihrem Beruf konfrontiert werden. Dann ist es gut, wenn Ihnen Privates nicht peinlich sein muss.
8. **Legen Sie Ihre Quellen offen.** Das zeugt von Respekt dem Urheber gegenüber und Sie gewinnen an Glaubwürdigkeit. Seien Sie sorgsam im Umgang mit Firmeninformationen! Sie dürfen beispielsweise keine vertraulichen Informationen verbreiten, die Sie im Rahmen Ihrer Anstellung erhalten (siehe Punkt 5 und den Hinweis am Ende des Leitfadens).
9. **Trennen Sie Meinungen und Fakten.** Um Missverständnisse zu vermeiden sollten Sie deutlich machen, welche Teile Ihrer Aussagen Meinungen und welche harte Fakten darstellen. Zudem sollten Sie darauf hinweisen, ob Sie Ihre persönliche oder die Unternehmensmeinung vertreten.
10. **Seien Sie ganz Sie selbst.** Vertrauen und Glaubwürdigkeit sind die Grundpfeiler sozialer Netze. Verstellen Sie sich nicht, sondern zeigen Sie wer und wie Sie sind. Zur offenen Kommunikation im Web 2.0 zählt auch, dass Sie Ihren Hintergrund offen legen. Wenn Sie für die [redacted] AG im Internet aktiv sind bzw. deren Interessen vertreten, stehen Sie dazu! Transparenz können Sie beispielsweise durch einen Disclosure-Hinweis (Disclaimer) sicherstellen, welcher an den Diskussionsbeitrag angehangen wird. Beispiel: *Ich arbeite für die [redacted] AG im Bereich [redacted]* oder *Ich bin Angestellter der [redacted] AG, vertrete hier jedoch meine eigene Meinung.*

Um die Einhaltung geltender Rechtsvorschriften in Ihrem eigenen sowie auch im Interesse der [redacted] AG sicher zu stellen, setzen Ihr Arbeitsvertrag, die Verhaltensrichtlinie (Integrity Code) sowie die Richtlinie zum Umgang mit Informationen verbindliche Grenzen. Das gilt insbesondere für den Umgang mit vertraulichen unternehmens- und personenbezogenen Informationen (siehe auch Punkt 5) sowie jedes Verhalten, das Sie einem Interessenkonflikt aussetzen kann.

[redacted]

Leiter Unternehmenskommunikation, [redacted] AG

Welcome to the World of Socialnomics

und

Vielen Dank für Ihre Aufmerksamkeit

Ihre Ansprechpartner

Ihre Ansprechpartner:

Dr. Florian Wäßle, LL.M.
Tel.: +49 69 247097 – 0
Mobil: +49 172 78 26 105
f.waessle@ac-tischendorf.com

Dr. Thomas Block
Tel.: +49 69 247097 – 0
Mobil: +49 160 90 828 104
t.block@ac-tischendorf.com

act | AC Tischendorf Rechtsanwälte

Zeppelinallee 77
60487 Frankfurt am Main

Telefon +49 69 24 70 97-0
Telefax +49 69 24 70 97-20

act@ac-tischendorf.com
www.ac-tischendorf.com

Dr. Florian Wäßle, LL.M.

Dr. Florian Wäßle, LL.M. berät deutsche und internationale Unternehmen in allen Fraugen des Informations- und Technologierechts, insbesondere im Software- und Lizenz-vertragsrecht sowie bei technologieorientierten Transaktionen und Outsourcing-Projekten. Er vertritt Mandanten in komplexen streitigen Auseinandersetzungen vor Gerichten sowie in internationalen und nationalen Schiedsgerichtsverfahren. Er verfügt über die Zusatzqualifikationen der Fachanwälte für gewerblichen Rechtsschutz sowie für Informationstechnologie. Florian Wäßle hat Rechtswissenschaften an den Universitäten Mannheim und Düsseldorf studiert. Vor seinem Eintritt bei AC Tischendorf Rechtsanwälte im Jahr 2003 war er für eine renommierte US-amerikanische Kanzlei in Frankfurt am Main tätig. Berufsbegleitend hat er einen Master of Laws (LL.M.) im Informations-recht erworben. Florian Wäßle publiziert regelmäßig in angesehenen Fachzeitschriften und ist Referent zahlreicher Vorträge in seinen Schwerpunktgebieten.

Dr. Thomas Block

Dr. Thomas Block berät eine Vielzahl von Unternehmen sowie Finanzinvestoren in speziellen Fragen des Arbeits- und Wirtschaftsrechts sowie bei Transaktionen. Dabei liegt sein Schwerpunkt neben der Begleitung des arbeitsrechtlichen Tagesgeschäfts in der Umsetzung komplexer arbeitsrechtlicher Fragestellungen, insbesondere im Zusammenhang mit Restrukturierungen. Er ist Partner bei AC • Tischendorf Rechtsanwälte und verfügt über die Zusatzqualifikation des Fachanwalts für Arbeitsrecht. Seine berufliche Karriere hat er - im Anschluss an seine juristische und fremdsprachenfach-spezifische Ausbildung in Münster, Frankfurt am Main und Caen - zunächst in einer führenden deutschen Arbeitsrechtskanzlei begonnen.