TAGUNG
CORPORATE MEDIA
GEZIELT. INNOVATIV. REALISIERBAR

DEUTSCHE PRESSEAKADEMIE
STUDIUM · SEMINARE · TAGUNGEN

Datenschutz und soziale (mobile) Medien

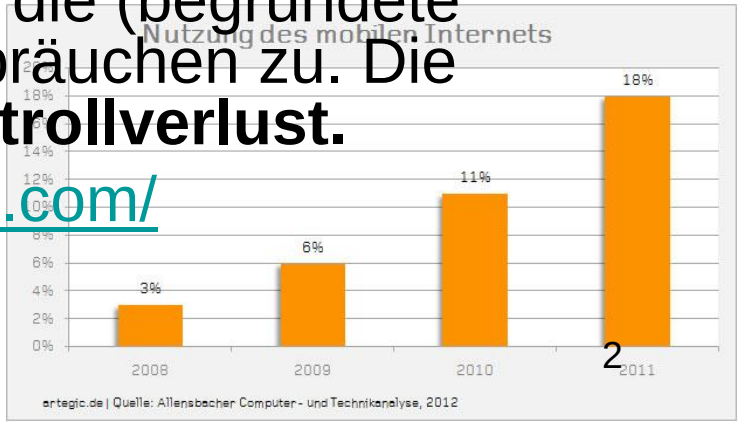
Jan Mönikes
Schalast&Partner Rechtsanwälte

Social Mobile Media

- Der Boom von internetfähigen Tabletts und Smartphones treibt soziale Medien – und umgekehrt.
- Die Nutzung sozialer Netzwerke auf mobilen Endgeräten in den EU5-Ländern – Deutschland, Frankreich, Großbritannien, Italien und Spanien – ist innerhalb eines Jahres um 44 Prozent angestiegen. Stärker wächst nur die mobile Nutzung von E-Mail-Diensten.

(Quelle: Cocom, artegic Studie - http://www.artegic.de/eCRM/DE/Aktuelles/Die-Mobile-Nutzung-von-Social-Media-waechst-in-Deutschland-und-Europa-deutlich_0cq-3zn.html)

- Mit der Verbreitung nimmt zugleich die (begründete wie unbegründete) Angst vor Missbräuchen zu. Die wesentliche Angst der Nutzer: **Kontrollverlust.**
- Beispiel: http://www.takethislollipop.com/



Mengen und Risikoproblem

- Vielen Anwendern ist es tatsächlich nicht bewusst, das beim Nutzen von (internetfähigen) Smartphones Daten in sehr großem Umfang anfallen. Diese Daten können ausgelesen und zu einem individuellen Profil zusammengeführt werden.
- Facebook, Google+, Gowalla, twitter und foursquare: Daten aus Handys und Smartphones können ein sehr genaues Bild über das (aktuelle wie vergangene) geografische Verhalten, den direkten Freundeskreis und sehr intime und vertrauliche Informationen vermitteln.
- Beispiel: http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten

Mengen und Risikoproblem

- Die Sorge ist: Immer mehr Stellen wissen über einen Bürger immer mehr – er darüber aber immer weniger und kann gegen negative Folgen nichts tun.
- Missbrauchsmöglichkeiten nehmen zu und werden immer einfacher.
- Die Gefahren von Belästigung und Täuschung, illegaler Nutzung und Datendiebstahl steigt.
- Andererseits: Als Verbraucher und Internetnutzer schätzen viele Menschen die neuen Möglichkeiten und geben freiwillig viele persönliche Daten von sich preis.

Gowalla

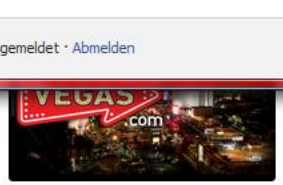
Have an account? Sign In

Discover our world's most loved places while sharing the places that mean the world to you.

Sign Up with Facebook

I don't have Facebook, but I would like to create a Gowalla account.

Browse Our Berlin Guide



from your friends, locals and experts

Social Media Services: Unersättliche Datenkraken?

- Während viele davor in der Tradition des Datenschutzes vor „**Datenfressern**“ warnen, bei denen „Internetfirmen und Staat sich unsere persönlichen Daten einverleiben“ (vgl. Constanze Kurz und Frank Rieger), gibt es zugleich auch eine Gegenbewegung: Die Diskussion um die “**Post-Privacy**” setzt den überkommenen Datenschutz unter Legitimationsdruck (vgl. Christian Heller).
- Das Konzept von Privatsphäre befindet sich im Wandel: Die **Diskrepanz** zwischen den Datenschutzforderungen und dem eigentlichen Verhalten der meisten Bürger im Internet ist offensichtlich.
- Die orwellsche Gesellschaft aus 1984 zum Beispiel – die wohl wichtigste Erzählung zur Verteidigung der Privatsphäre – zeichnet sich zudem in der Tat nicht nur durch Überwachung aus. Mindestens eben so wichtig ist die Vereinzelung und die Kontrolle der Informationsflüsse der Menschen untereinander. Wer abgeschottet von einander lebt, kann sich nicht gegen die Macht organisieren.
- Das Konzept „Datenschutz“ kann also auch Basis einer Macht sein, die darauf baut, den vertikalen Informationsfluss zu gewährleisten, indem sie die horizontale Durchlässigkeit eindämmt.

Datenschutz für Deutsche wichtig

- Aber: Für 81 Prozent der Deutschen ist der Schutz der persönlichen Daten ein **zentrales Thema**. (TNS Emnid im Auftrag der CPP GmbH).
- Wenn es jedoch um Vertrauen erweckende Unternehmen beim Datenschutz geht, denken nur 26 Prozent der Bundesbürger an ihren Mobilfunk- oder Internetanbieter. Im Ranking der vertrauenswürdigsten Institutionen liegen Telekommunikationsanbieter an drittletzter Stelle vor dem Versandhandel (25 Prozent) und Social-Media-Netzwerken (8 Prozent).
- Quelle: http://www.mobilebusiness.de/nc/home/news-detail/article/sind-handy-und-internetanbieter-vertrauenswuerdig.html

Ziel: Schutz des Persönlichkeitsrechts

- Ziel des Datenschutzes ist der **Schutz vor Rechtsverletzungen** und der „**informationellen Selbstbestimmung**“ als Teil des allg. Persönlichkeitsrechts (Art.1, 2 GG).
- Schutz des Einzelnen vor Verletzung seines Persönlichkeitsrechts beim **Umgang** mit seinen personenbezogenen Daten (§1 Abs. 1 BDSG)
- Wahrung des Persönlichkeitsrechts bei der **Verarbeitung** von personenbezogenen Daten (§ 1 Abs. 1 BDSG, Volkszählungsurteil BVerfG 1983)
- Recht auf **Integrität und Vertraulichkeit informationstechnischer Systeme** (BVerfG 2008 zur heiml. Onlinedurchsuchung)

Andere Technik – gleiches Recht

- Viele Probleme für die Anbieter von Mobile-Commerce und mobile (social) Media sind dem Umstand geschuldet, dass Gesetze und Rechtsprechung **keinen Unterschied** machen zwischen Verträgen, die über einen PC oder ein Smartphone geschlossen werden. Die beim M-Commerce verwendete Technik kann also nicht als Ausrede dienen, wenn es darum geht, rechtliche Probleme zu umgehen oder zu lösen.
- Denn: Rechtlich besteht **kein Unterschied** zwischen M-Commerce und E-Commerce. In jedem Fall sind z.B. Impressum, AGBs usw. entsprechend der allgemeinen Regeln abrufbar zu halten.
- Das bedeutet, dass die rechtlichen Anforderungen, die das Gesetz beispielsweise an einen Webshop für Spielzeug stellt, dieselben sind, die an einen Händler gestellt werden, der auch über eine App Spielzeug vertreiben will.
- Die Größe des Bildschirms und andere technischen Probleme zu überwinden, ist eine tatsächliche Hürde, die das Recht ignoriert.
- Andererseits kommen durch die Integration verschiedenster Anwendungen in ein Gerät neue (rechtliche) Herausforderungen hinzu, die es zu bewältigen gilt.

Grundsätze des Persönlichkeitsschutz

- Verarbeitung von personenbezogenen Daten nur, wenn eine Rechtsnorm dieses **erlaubt** oder der Betroffene **eingewilligt** hat (§ 4 Abs. 1 BDSG, Verbot mit Erlaubnisvorbehalt)
- Prinzip der Datenvermeidung und Datensparsamkeit (§ 3a BDSG)
- Datenerhebung nur vom Betroffenen
- Unterrichtung des Betroffenen über Zweck der Verarbeitung, eventuelle Übermittlungen und ggfs. über die Freiwilligkeit seiner Angaben
- Zweckbindung der Datenverarbeitung
- Auskunfts- Berichtigungs- und Löschungsrecht

Anwendungsbereich

- Datenschutz gilt für **alle** privatwirtschaftlichen und öffentlichen Stellen für die Verarbeitung von personenbezogenen Daten (§ 3 Abs. 1 BDSG)
  - durch Datenverarbeitungsanlagen jeder Art
  - in jeder Form automatisierten Verfahrens (Datenbanken, Dateien, Tabellen)
- Personenbezogene Daten sind Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen lebenden Person (§ 3 Abs. 1 BDSG), z.B. Kunden-, Lieferanten-, Mitarbeiterdaten.

Technische Ebene des Datenschutz

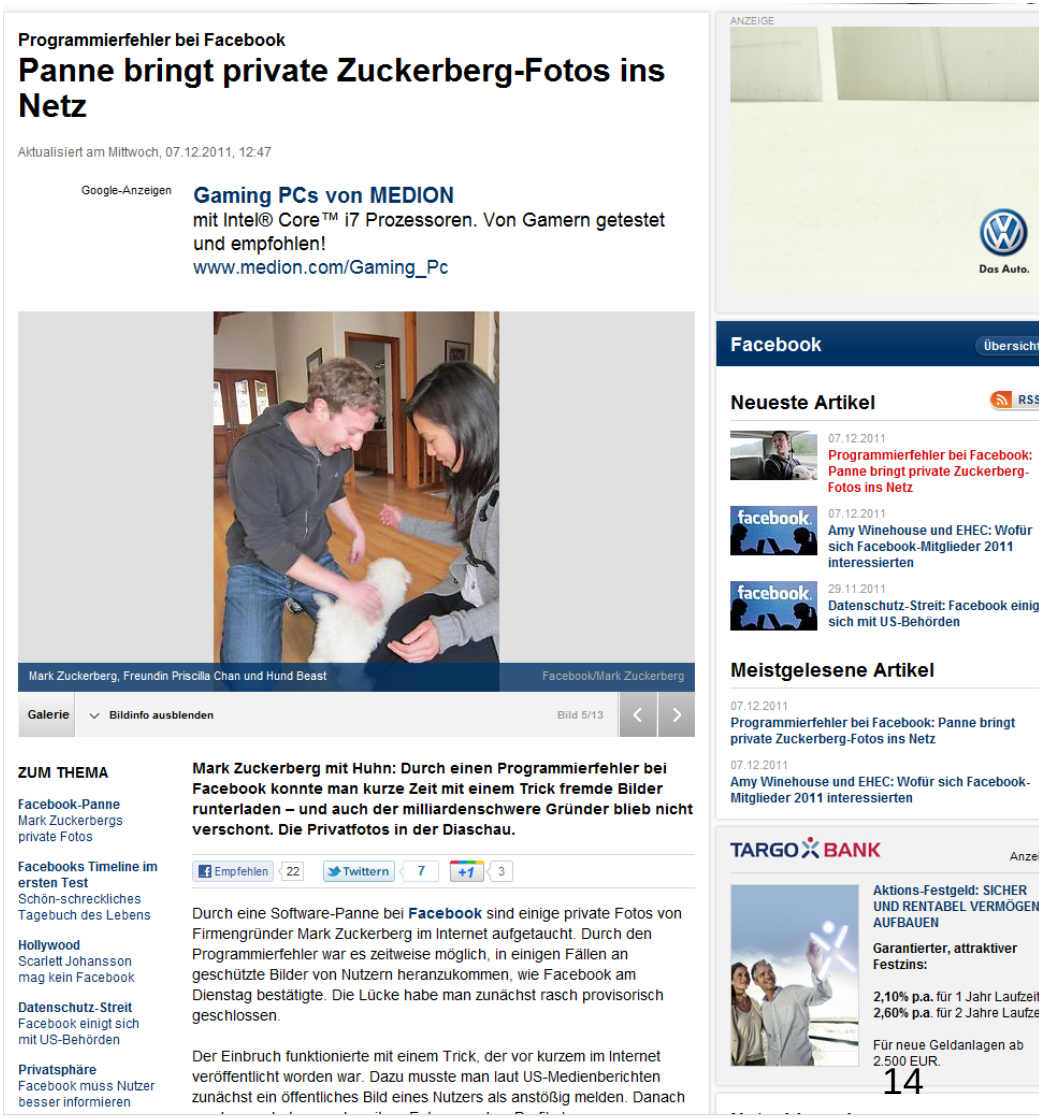
- Schutz vor
  - unberechtigter Kenntnisnahme oder Einsichtnahme (Vertraulichkeit)
  - zufälliger Zerstörung, Gewährleistung der Nutzungsmöglichkeiten (Verfügbarkeit)
  - unberechtigter Veränderung, Gewährleistung der Richtigkeit und Vollständigkeit (Integrität)
- Nachweis der Urheberschaft und der Echtheit digitaler Dokumente (Authentizität)
- Nachweis, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit).

Umgang mit Kundendaten

- Zur Ausführung des Vertrages mit dem **eigenen** Kunden ist jede **nötige** Datenverarbeitung zur Wahrnehmung der Rechte und Pflichten des Vertrages gestattet (aber auch nur diese).
- Umfasst sind diesbezüglich auch sonstige Nutzungen wie Warndateien, Übermittlung an Auskunfteien, Bonitätsprüfung, Kundenbefragungen und Bestandswerbung, Datenanalysen, etc.
- Daten aus allg. zugänglichen Quellen dürfen ebenfalls hinzugespeichert werden (§ 28 Abs. 3 S. 3 BDSG), soweit es zulässige Quellen sind und keine schutzwürdigen Interessen des Betroffenen verletzt werden.

Datensicherheit

- Während die Verarbeitung von Daten in sozialen Medien in der Öffentlichkeit vor allem „nur“ Unwohlsein erzeugt, können Probleme bei der Datensicherheit von Kundendaten dagegen existentiellen Vertrauensverlust zur Folge haben.
- Besonders Unternehmen, die Daten für Dritte verarbeiten, müssen daher auf hinreichende Datensicherheit garantieren und auch die diesbezügl. Bestimmungen des BDSG einhalten.



Programmierfehler bei Facebook

Panne bringt private Zuckerberg-Fotos ins Netz

Aktualisiert am Mittwoch, 07.12.2011, 12:47

Google-Anzeigen

Gaming PCs von MEDION
mit Intel® Core™ i7 Prozessoren. Von Gamern getestet und empfohlen!
www.medion.com/Gaming_Pc

Mark Zuckerberg, Freundin Priscilla Chan und Hund Beast — Facebook/Mark Zuckerberg

Galerie — Bildinfo ausblenden — Bild 5/13

ZUM THEMA

Facebook-Panne
Mark Zuckerbergs private Fotos

Facebooks Timeline im ersten Test
Schön-schreckliches Tagebuch des Lebens

Hollywood
Scarlett Johansson mag kein Facebook

Datenschutz-Streit
Facebook einigt sich mit US-Behörden

Privatsphäre
Facebook muss Nutzer besser informieren

Mark Zuckerberg mit Huhn: Durch einen Programmierfehler bei Facebook konnte man kurze Zeit mit einem Trick fremde Bilder runterladen – und auch der milliardenschwere Gründer blieb nicht verschont. Die Privatfotos in der Diaschau.

Empfehlen 22 — Twittern 7 — +1 3

Durch eine Software-Panne bei **Facebook** sind einige private Fotos von Firmengründer Mark Zuckerberg im Internet aufgetaucht. Durch den Programmierfehler war es zeitweise möglich, in einigen Fällen an geschützte Bilder von Nutzern heranzukommen, wie Facebook am Dienstag bestätigte. Die Lücke habe man zunächst rasch provisorisch geschlossen.

Der Einbruch funktionierte mit einem Trick, der vor kurzem im Internet veröffentlicht worden war. Dazu musste man laut US-Medienberichten zunächst ein öffentliches Bild eines Nutzers als anstößig melden. Danach

ANZEIGE

Das Auto.

Facebook — Übersicht

Neueste Artikel — RSS

07.12.2011
Programmierfehler bei Facebook: Panne bringt private Zuckerberg-Fotos ins Netz

07.12.2011
Amy Winehouse und EHEC: Wofür sich Facebook-Mitglieder 2011 interessierten

29.11.2011
Datenschutz-Streit: Facebook einig sich mit US-Behörden

Meistgelesene Artikel

07.12.2011
Programmierfehler bei Facebook: Panne bringt private Zuckerberg-Fotos ins Netz

07.12.2011
Amy Winehouse und EHEC: Wofür sich Facebook-Mitglieder 2011 interessierten

TARGOBANK — Anzei

Aktions-Festgeld: SICHER UND RENTABEL VERMÖGEN AUFBAUEN

Garantierter, attraktiver Festzins:

2,10% p.a. für 1 Jahr Laufzeit
2,60% p.a. für 2 Jahre Laufze

Für neue Geldanlagen ab 2.500 EUR.

Werbung mit Listendaten

- **Briefwerbung** kann mit sog. Listendaten betrieben werden.
- Listendaten (§ 28 Abs. 3 Satz 2 BDSG)
  - Art der Personengruppe
  - Berufs-, Branchen- oder Geschäftsbezeichnungen
  - Name, Titel, akad. Grad
  - Anschrift
  - Geburtsjahr
- Bei Daten von Kunden oder Interessenten (z.B. aus verbindlichen Angeboten) oder aus allg. zugänglichen Verzeichnissen dürfen Daten aus anderen zulässigen Quellen hinzugespeichert und genutzt werden (z.B. zur Zielgruppenselektion).
- Die Verwendung dieser Daten B2C ist nur ausnahmsweise ohne Einwilligung zulässig (§ 28 Abs. 3 S. 2 BDSG)
  - Eigener Kundenstamm
  - Aus allg. zugänglichen Verzeichnissen (Internet Adresslisten – nicht: Suchmaschinenergebnisse)
- Die Verwendung B2B ist auch ohne Einwilligung zulässig
  - Wenn die Daten aus anderen legalen Quellen erhoben wurden und die betrieblichen Adressdaten verwendet werden.

Allgemeine Werbe-Regeln

- Unabhängig von der Zielgruppe:
  - Bei jeder Ansprache durch Brief ist der Betroffene über das jederzeitige Widerspruchsrecht zu unterrichten (28 Abs. 4 Satz 2 BDSG).
  - Eventuell schutzwürdige Interessen des Betroffenen müssen berücksichtigt werden.
- „Robinsonliste“ führen und beachten
- In gemischten Datenbeständen Zielgruppenzugehörigkeit kennzeichnen (B2B, B2C)
- Herkunft der Daten mit Datum, Art und Bearbeiter protokollieren.
- **Achtung:** Einwilligung zur Datenverarbeitung und Einwilligung zum Erhalt von Werbung sind unterschiedlich zu behandeln!

Telefonwerbung

- Aufgrund von § 7 UWG bei Privatkunden nur nach vorheriger Einwilligung zulässig
- Bei Geschäftskunden nur nach vorheriger Einwilligung oder wenn eine mutmaßliche Einwilligung unterstellt werden kann
- E-Mail-Einwilligung reicht **nicht** aus (auch nicht double-opt-in).
- Automatische Anrufansagen sind **nicht** zulässig.
- Die Rufnummer des Anschlusses muss übermittelt werden – Rückrufmöglichkeit muss dagegen nicht bestehen.

Goldene Regeln der Online-Werbung

Elektronische Werbung nach § 7 UWG nur mit vorheriger Einwilligung erlaubt (Spam-Verbot):

1. Nur explizit selbst angeforderte Werbung
2. Anmeldung per E-Mail nur per „double opt-in“ oder wenigstens „confirmed opt-in“
3. Verwendung von Adressen nur zum angegebenen Zweck
4. Der Empfänger müssen sich selbst vom Verteiler streichen können
5. Kündigungsmöglichkeit in jeder Mail
6. Keine Adressweitergabe ohne Zustimmung
7. Erläuterung des Umgangs mit personenbezogenen Daten

Verantwortlichkeit

- Betreiber von (mobilen) Angeboten, Internetanwendungen, Apps usw. sind Diensteanbieter i.S.v. § 12 TMG und verantwortliche Stelle i.S.v. § 3 Abs. 7 BDSG
- Von Nutzern eingegebene Daten wie z.B. E-Mail-Adressen und Namen sind persönliche Daten i.S.v. § 3 Abs. 1 BDSG
- Diese Daten dürfen grundsätzlich nicht ohne die Einwilligung des Nutzers weiterverwendet werden (z.B. an Dritte übertragen, an anderer Stelle wiedergegeben)
- Nutzer haben Rechte auf Auskunft (§ 34 BDSG) bzw. Berichtigung, Löschung oder Sperrung (§ 35 BDSG)

Besondere Sorgfaltspflichten

- Neben den Regeln des Datenschutzes können sich (datenschutz-) rechtlich auch aus weiteren Gründen besondere Verpflichtungen zu besonderer Sorgfalt im Umgang mit Daten ergeben.
- Beispiele sind:
  - Vertragliche Vereinbarungen und Garantien
  - Vertragliche (Neben-) Pflichten
  - Gesetzliche Geheimhaltungsverpflichtungen - Beispiel § 203 StGB, Ärztliche Schweigepflicht

Neue Möglichkeiten

http://www.youtube.com/watch?v=LMU8pdHj4pk

Alte Grenzen

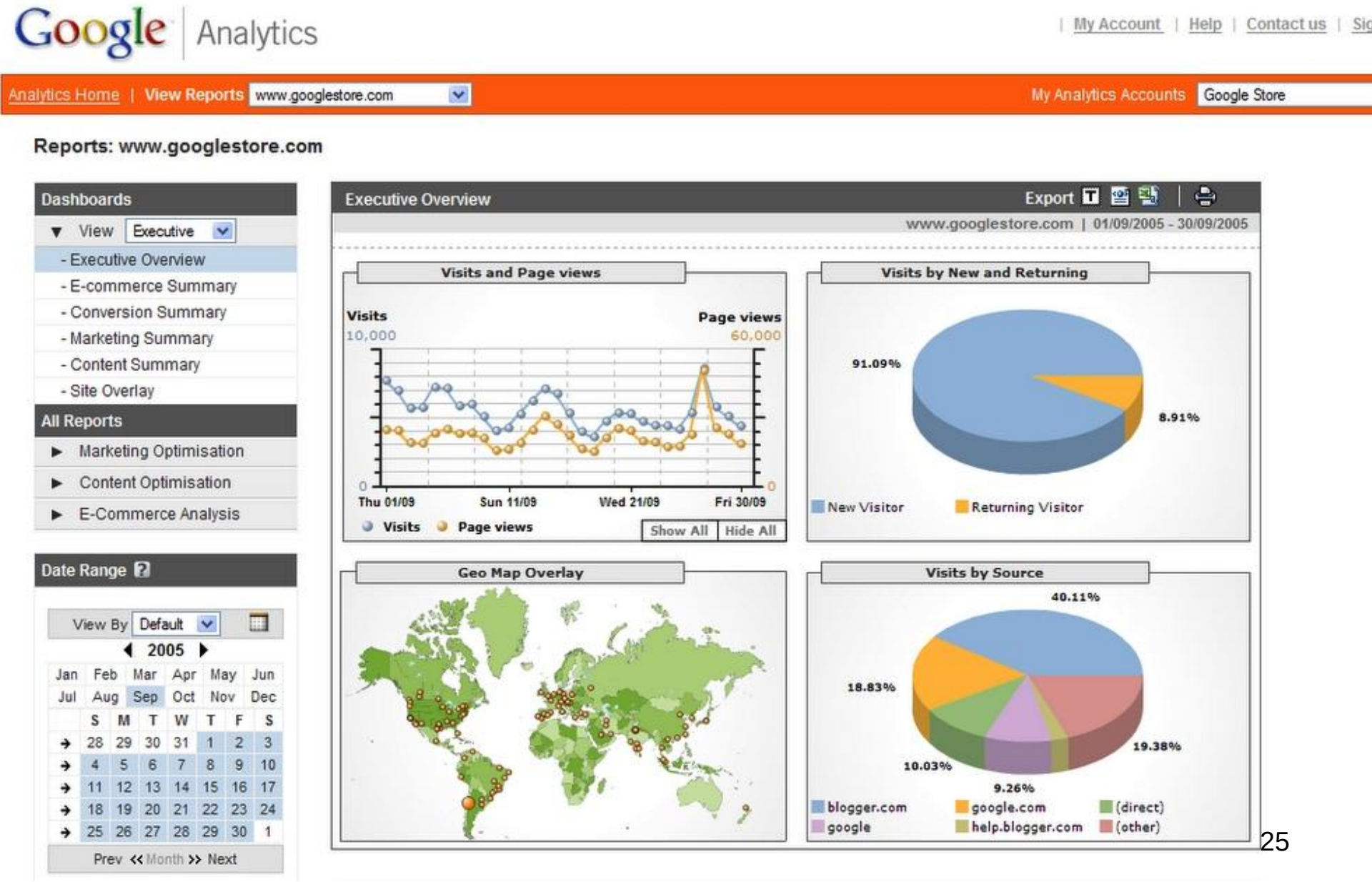
- Nach dem Datenschutzrecht dürften Daten, aus denen u. a. religiöse und weltanschauliche Überzeugungen, politische Meinungen, die Gesundheit oder das Sexualleben hervorgehen, **nur** dann verarbeitet werden, wenn eine besondere Rechtsvorschrift dies vorsieht oder der Betroffene einwilligt. (§§ 3 Abs. 9, 28 Abs. 6 BDSG)
- Die hier gezeigte Anwendung wären daher in dieser Form voraussichtlich in Deutschland insgesamt unzulässig.

Einwilligung

- Die Einwilligung muss sowohl in materieller als auch in formeller Hinsicht geeignet sein, zu einer datenschutzrechtlich zulässigen Datenverarbeitung führen zu können. **Anforderungen an die Einwilligungserklärung** lassen sich aus § 4a BDSG entnehmen, des Weiteren ist im Bereich der elektronischen Informations- und Kommunikationsdienste der strengere § 13 TMG zu beachten.
- Gemäß § 4a BDSG ist die Einwilligung des Betroffenen nur dann wirksam, wenn sie auf einer **freien Entscheidung** des Betroffenen beruht, d.h. der Betroffene seine Einwilligung bewusst und eindeutig erteilt hat.
- Er ist grundsätzlich zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten zu **unterrichten** und auf die Folgen der Verweigerung der Einwilligung hinzuweisen.
- Darüber hinaus bedarf die Einwilligung der Schriftform, wobei nach dem TMG auch eine Einwilligung auf elektronischem Wege möglich ist, sofern „der Diensteanbieter sicherstellt, dass
  - der Betroffene seine Einwilligung bewusst und eindeutig erteilt hat,
  - die Einwilligung protokolliert wird,
  - der Betroffene den Inhalt der Einwilligung jederzeit abrufen kann und
  - der Betroffene die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann."

Einwilligung

- Die Einwilligungserklärung muss auch optisch von anderen Erklärungen abgesetzt und diesen gegenüber hervorgehoben gestaltet sein.
- Sie ist außerhalb der Anwendbarkeit des TMG grundsätzlich schriftlich – also durch Unterschrift – zu erteilen.
- Eine **elektronische Einwilligung** nach § 13 Abs. 2 TMG ist **nur wirksam**, wenn der Nutzer sie durch ein Opt-In, also eine aktive Handlung, wie das **Anhaken eines Kontrollkästchens** bestätigt hat.



Im Zentrum: Die IP-Adresse

- Es ist höchst umstritten, ob es sich bei der IP-Adresse um ein personenbezogenes Datum handelt, das den Anwendungsbereich des BDSG eröffnet. Der Diskussionsstand befindet sich insoweit auch weiterhin im Fluss. Dabei steht das Merkmal der „Bestimmbarkeit“ im Vordergrund.
- Vielfach wird für eine „relative“ Betrachtungsweise plädiert: Ein und dasselbe Datum kann nach dieser Auffassung bei der einen verantwortlichen Stelle (vgl. § 3 Abs. 7 BDSG) aufgrund ihrer Nachforschungsmöglichkeiten ein personenbezogenes Datum sein und bei einer anderen Stelle nicht.

Personenbeziehbar = Personenbezogen?

- In § 3 Abs. 1 BDSG wird bestimmt:
- *Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)*
- Art. 2 a) der EU-Datenschutzrichtlinie bestimmt:
- *alle Informationen über eine bestimmte oder bestimmbare natürliche Person ("betroffene Person"); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind*
- Ein personenbezogenes Datum liegt also dann vor, wenn eine Person **bestimmbar** ist, wofür es nach der Richtlinie soagr ausreicht, dass die Person indirekt identifiziert werden kann.
- Bei dynamischen IP-Adressen kann zumindest mithilfe des Zugangsproviders ermittelt werden, welche Person Anschlussinhaber bzw. Kunde des Providers ist. Dass es sich hierbei nicht um ein theoretisches Szenario handelt, zeigen die vielen Fälle von illegalen Filesharing, in denen in jedem Jahr mehrere hunderttausend Anschlussinhaber identifiziert und anschließend abgemahnt werden.

Personenbeziehbar = Personenbezogen?

- Die Gegenauffassung lehnt daher – meist unter pauschalem Hinweis auf den Grundrechtsschutz der Betroffenen – jegliche Relativierung ab und lässt es ausreichen, dass (theoretisch-abstrakt) Möglichkeiten denkbar sind, die das Datum mit einer natürlichen Person in Verbindung bringen.
- Zudem ist zwischen statischen und dynamischen Adressen zu unterscheiden: Eine feste (statische) IP-Adresse, mit der sich jeder Rechner bei der Kommunikation im Internet identifiziert, bestimmt in der Regel dessen Inhaber, begründet mithin Personenbezug, falls dies eine natürliche Person ist.
- Während statische IP-Adressen bisher im Wesentlichen dem professionellen Bereich vorbehalten waren, ist unter dem neuen Internet-Protokoll IPv6 wohl eine generelle Verwendung absehbar.
- Die bisher weit überwiegend verwendeten, vom Service-Provider pro Wählverbindung vergebenen dynamischen IP-Nummern, sind wohl jedenfalls für diesen personenbezogen, da er anhand der von ihm in der Regel geführten Bestands- und Verbindungsdaten die Zuordnung zum Inhaber des Rechners vornehmen kann.

Personenbeziehbar = Personenbezogen?

- Für die in den Logfiles der Anbieter von Telemediendiensten, so von Webseitenbetreibern oder Suchmaschinen, enthaltenen mit IP-Adressen verknüpften Daten über die Internet-Nutzung ist der Personenbezug nur nach der strengeren Auffassung zu bejahen. Selbst wenn dazu auf Daten eines Dritten zurückgegriffen werden müßte.
- Das gelte auch, wenn zur Zuordnung weitere Angaben seitens des Betreibers einer Firewall o.Ä. herangezogen werden müssen (Auskünfte des IP-Providers seien bspw. über § 101 Abs. 2 UrhG zu erreichen). Da diese Auskünfte aber an Bedingungen geknüpft sind, betrachtet die Gegenmeinung das Zusatzwissen als grundsätzlich nicht legal zugänglich und damit den Aufwand als **unverhältnismäßig**.
- Dem wird jedoch wiederum entgegengehalten, dass wegen der breiten Streuung der IP-Adresse während einer lang andauernden Session (flatrate) unter oft hunderten von Anbietern besuchter Seiten, von denen eine Vielzahl die Identität des Betroffenen kennen würden und die wegen entsprechender Nutzungsbedingungen oder ihres Standorts in Drittländern faktisch oder rechtlich nicht gehindert seien, diese weiterzugeben, die Personenbestimmung nicht mit so hoher Wahrscheinlichkeit ausgeschlossen werden könne oder der Aufwand unverhältnismäßig erscheine.

Save Harbour

- Beim Datenexport in die USA galt, dass ein Unternehmen in den USA dann ein „angemessenes Datenschutzniveau“ gemäß §§ 4b, 4c BDSG aufweist, wenn es dem **Safe-Harbour Abkommen** beigetreten war.
- Der **Düsseldorfer Kreis** (ein Zusammenschluss der deutschen Datenaufsichtsbehörden für nicht-öffentliche Stellen) hat jedoch im April 2010 beschlossen, dass er die Safe-Harbour Zertifizierung alleine **nicht mehr** für ausreichend anerkennt. Grund für diesen Beschluss war, dass einige Unternehmen in den USA angaben, über eine Safe-Harbour Zertifizierung zu verfügen, ohne dass dies der Fall war. Zudem fand in den USA praktisch keine Kontrolle statt, ob die Safe-Harbour-Prinzipien von den angeschlossenen Unternehmen eingehalten werden. Schließlich wurden größere Defizite im Bereich Datenschutz in den USA dokumentiert.
- Um zu gewährleisten, dass das „angemessene Datenschutzniveau“ tatsächlich im betreffenden US-Unternehmen gegeben ist, muss sich das datenexportierende deutsche Unternehmen nach dem Beschluss des Düsseldorfer Kreises nun **schriftlich nachweisen lassen**, dass das US-Unternehmen dem Safe-Harbour Abkommen beigetreten ist. Dabei dürfen der Nachweis bzw. die Zertifizierung **nicht älter als sieben Jahre** sein.

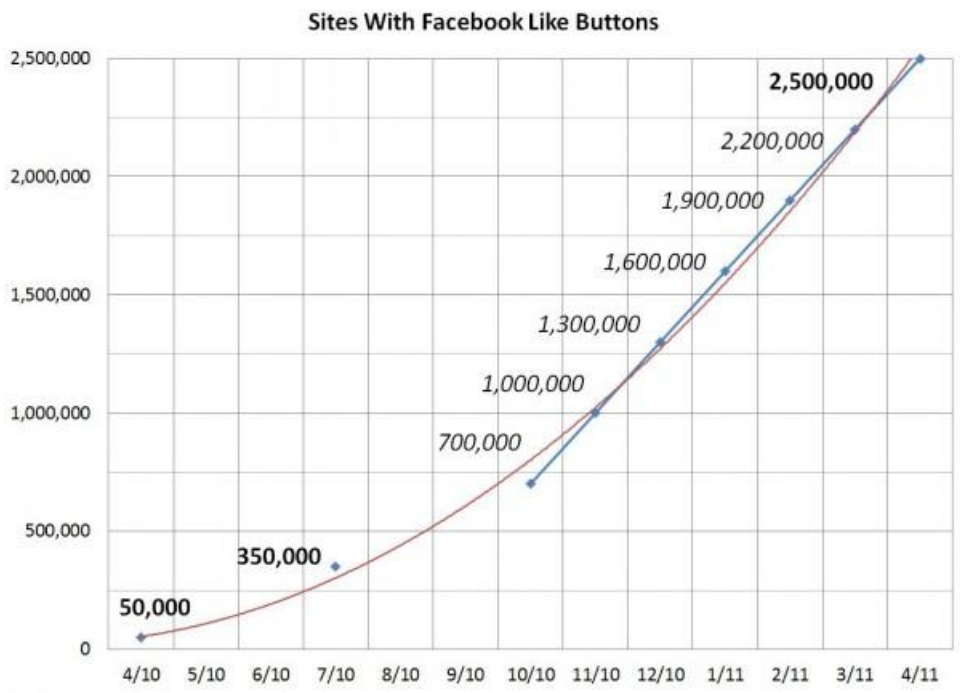
Save Harbour

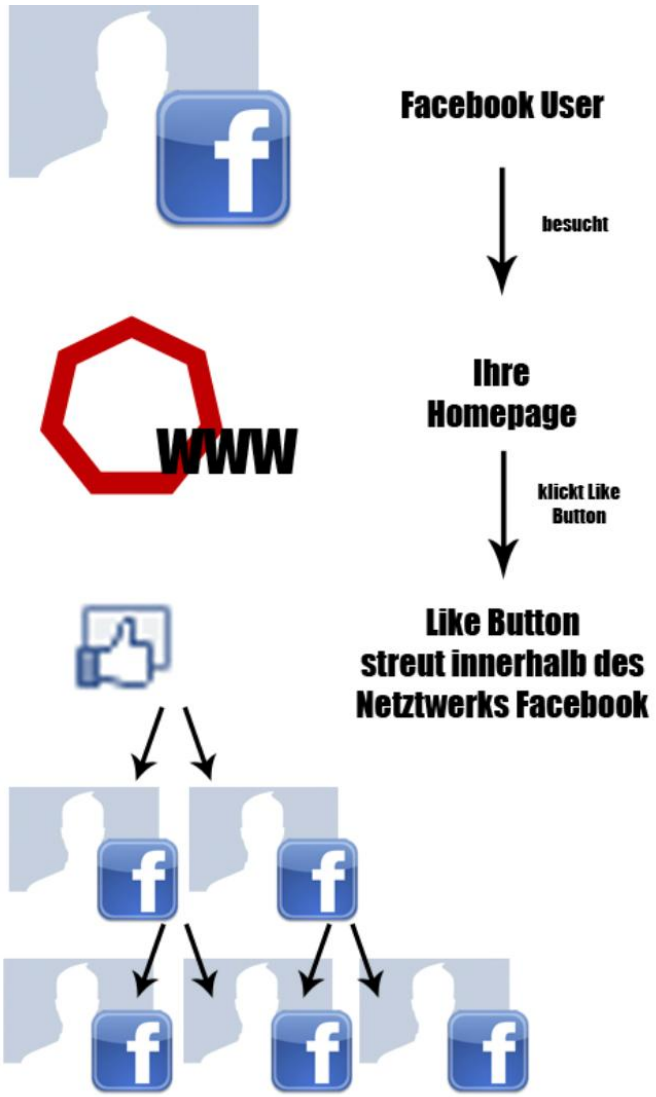
- Ferner muss sich das deutsche Unternehmen nachweisen lassen, dass und wie die Safe-Harbour-Grundsätze, insbesondere die Informationspflichten gegenüber den Betroffenen, **eingehalten** werden. Da das deutsche Unternehmen auf Verlangen der Aufsichtsbehörde die entsprechenden Nachweise vorlegen muss, sind diese entsprechend zu **dokumentieren**.
- Falls das deutsche Unternehmen diesen Verpflichtungen **nicht** nachkommt, drohen Bußgelder bis zu 300.000 Euro.
- Falls diese Nachweise vom US-Unternehmen **nicht** erbracht werden können, besteht immer noch die Möglichkeit, die Datenübermittlung **auf Basis der EU-Standardvertragsklauseln vertragsrechtlich** auszugestalten (bzw. Vertrag über die Auftragsdatenverarbeitung gem. § 11 BDSG).
- Diese gewähren auch ein „angemessenes Datenschutzniveau“, so dass die Datenübermittlung in die USA oder in andere Staaten, wie beispielsweise Indien, rechtlich zulässig gestaltet werden kann.

Cloud Computing

- Beim Cloud Computing ist die zentrale Frage stets, welches nationale Datenschutzrecht überhaupt Anwendung findet:
- Werden Daten durch eine verantwortliche Stelle mit Sitz in einem anderen Mitgliedstaat der EU oder des EWR in Deutschland erhoben, verarbeitet oder genutzt, ist das BDSG nicht anwendbar. Ausnahme: Hat das jeweilige Unternehmen jedoch eine Niederlassung in Deutschland, gilt das BDSG weiterhin. Interessant ist in diesem Zusammenhang auch die Frage, ob ein in Deutschland betriebenes Rechenzentrum bereits als Niederlassung zu werten ist, was wohl zu bejahen ist.
- Für Unternehmen außerhalb der EU bzw. des EWR gilt das Territorialprinzip, so dass bei einer Erhebung, Speicherung oder Nutzung von Daten auf deutschem Territorium das BDSG anwendbar bleibt.
- Der Einsatz von Clouds bringt eine Vielzahl von juristischen Herausforderungen mit sich, so dass sich hier stets die Einzelfallprüfung durch einen Experten empfiehlt.


Like


Sites With Facebook Like Buttons
2,500,000
2,000,000
1,500,000
1,000,000
500,000
0
4/10
5/10
6/10
7/10
8/10
9/10
10/10
11/10
12/10
1/11
2/11
3/11
4/11
50,000
350,000
700,000
1,000,000
1,300,000
1,600,000
1,900,000
2,200,000
2,500,000


Facebook User
besucht
WWW
Ihre Homepage
klickt Like Button
Like Button streut innerhalb des Netztwerks Facebook

Prinzip des Like-Buttons

- Für den Like-Button bindet die Web-Seite einen sogenannten iFrame ein. Dabei sendet der Browser an Facebook unter anderem als Referer die URL der gerade geöffneten Seite. Außerdem schickt er dem Facebook-Server auch das von ihm bereits früher gesetzte Cookie. Ist der Anwender gerade in einem anderen Fenster bei Facebook angemeldet, enthält das seine Sitzungs-ID. Damit kann Facebook den Aufruf einer Seite ggfs. **einer konkreten Person** zuordnen.
- Facebook kann also, während man in Facebook angemeldet ist, beobachten, welche Web-Seiten der Nutzer aufruft, sofern diese einen solchen Like-Button oder andere Facebook-Elemente enthalten.
- Auch wer **nicht** bei Facebook angemeldet ist, übermittelt anscheinend Daten an deren Server. Da der Browser das von Facebook gesetzte Cookie bei jeder Verbindung mit einem Facebook-Server ungefragt mitschickt, könnte der Betreiber damit prinzipiell ein Profil erstellen, welche Web-Seiten der zu der Kennung gehörende Anwender aufgerufen hat. Und es wäre dann auch durchaus möglich, diese Kennung später – etwa beim späteren Anmelden bei Facebook – auch wieder einer Person zuzuordnen.

Argumentation des UDL contra Facebook

- Durch den Dienst „Facebook Insight“, der bei Fanpages und den Social-Plugins zum Einsatz kommt, werden personenbezogene Daten erhoben und verarbeitet.
- Daneben werden auch bei der Nutzung von externen Diensten und den Fanpages Angaben mit Personenbezug erhoben und verarbeitet.
- Dazu gehört die IP-Adresse (EU und Dt. Datenschutz-Aufsichtsbehörden: hat Personenbezug).

Personalisierung durch Cookies

- Außerdem nutzt Facebook **Cookies**, mit denen Nutzerinnen und Nutzer individualisiert werden können.
- Und: Facebook erhebt und verarbeitet weitere Angaben, die zu einer umfassenden Profilierung des jeweiligen Nutzers führen.
- Im Zusammenhang mit den durch die Nutzerinnen und Nutzer eingestellten Informationen ergeben sich somit Persönlichkeitsprofile, deren Detaillierungsgrad je nach Intensität der Nutzung von Facebook oder der Angebote, die Social-Plugins von Facebook einsetzen, variiert.

Verantwortlichkeit der Website

- Ist die Website, die das iFrame zu Facebook gesetzt hat, dafür verantwortlich?
- Verantwortliche Stelle ist gemäß § 3 Abs. 7 BDSG die Stelle, die „personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt“, bzw. nach Art. 2 Buchst. d) S. 1 EU-DSRL die Stelle, „die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“.
- Für Diensteanbieter von Telemedien gelten die §§ 2 S. 1 Nr. 1, 3 Abs. 1 TMG.

Anwendbares Recht

- Territorialitätsprinzip: Der Ort der Datenverarbeitung bestimmt, welches nationale Datenschutzrecht anwendbar ist.
- Stammsitz von Facebook in Kalifornien (USA) in der EU in Dublin (Irland)
- Da Facebook in Irland eine verantwortliche Niederlassung betreibt und keine Niederlassung in Deutschland besteht, ist für die Datenverarbeitung von Facebook zwar gemäß den gesetzlichen Zuständigkeitsregelungen irisches Recht anwendbar (§ 3 Abs. 1 u. 3 Nr. 4 TMG i. V. m. § 1 Abs. 5 BDSG).
- Aber: Facebook Irland dient nur als Anlauf- und Beschwerdestelle; nur hierfür ist dann irisches Datenschutzrecht anwendbar.
- Anwendbarkeit des TMG: § 3 Abs. 1 TMG (Herkunftsland)
- § 1 Abs. 5 TMG: daneben Anwendung der jeweiligen privatrechtlichen Kollisionsregeln: haben Telemedienanbieter Töchter/ Filialen in Deutschland und **zielt deren Angebot auf den deutschen Markt**, z. B. indem ein deutschsprachiges Angebot bereitgehalten wird, so verfolgen diese Unternehmen gezielt die Erhebung und Verarbeitung von deutschen Nutzerdaten.
- In diesem Fall kann bei einer außereuropäischen Datenverarbeitung an die Verarbeitung auf den Nutzerrechnern (z. B. durch Setzen von Cookies) angeknüpft werden, und deutsches Recht ist anwendbar.
- Hinsichtlich der Datenverarbeitung des Sozialen Netzwerks Facebook selber, ist Facebook Inc. Betreiber bzw. die Facebook GmbH in Hamburg verantwortliche Stelle. Damit ist für die Datenverarbeitung von Facebook wieder direkt deutsches Datenschutzrecht anwendbar.

Facebook

- Facebook ist
  - zugleich
    - Diensteanbieter für kommerzielle Kommunikation (§ 2 S. 1 Nrn. 1, 5 TMG),
    - Anbieter von Telekommunikationsdiensten für den Bereich der Telekommunikation (§ 3 Nrn. 6, 24 TKG)
  - und somit datenverarbeitende Stelle i. S. d. BDSG und der EU-DSRL.

Einbindung in Website?

- Bei Facebook-Fanpagebetreibern und Webseitenbetreibern mit Sitz in Deutschland handelt es sich durchgängig um Diensteanbieter von Telemedien, auf die das TMG anwendbar ist.
- Sie sind datenschutzrechtlich **verantwortlich für die über ihre Webseite vorgenommene Verarbeitung personenbezogener Daten.**
- Auch soweit ein Webseitenbetreiber externe Dienstleister in Anspruch nimmt, kann er sich der datenschutzrechtlichen Verantwortung für die durch und über das Angebot vorgenommene Verarbeitungen und angestoßenen Prozesse nicht entziehen.

Störerhaftung?

- Social-Plugins von Facebook auf der Webseite eines Drittanbieters haben zur Folge, dass bei deren Verwendung eine direkte Kommunikation zwischen dem Rechner des Nutzenden und Facebook aufgebaut wird.
- Eine **direkte** Datenerhebung und -speicherung durch den Webseitenbetreiber erfolgt nicht.
- Dies ändert jedoch nichts an der Verantwortlichkeit des Webseitenbetreibers, der durch die Gestaltung seiner Webseite die Datenweitergabe an Facebook initiiert und in der Hand hat.
- Dieses ist ihm im Sinne der allgemeinen Zurechnungsregeln auch zurechenbar (Störerhaftung).

Reichweitenanalyse

- **Untrennbar** mit dem Einsatz von Social-Plugins ist die Erstellung einer Reichweitenanalyse zugunsten des Diensteanbieters verbunden (Facebook Insights).
- Geregelt: § 15 Abs. 3 TMG
- Verantwortlicher für die Nutzung der personenbezogenen Daten: bei Diensteanbieter (der zur Erfüllung dieser Aufgabe einen Dienstleister, im konkreten Fall Facebook, heranzieht)
- Nutzer im datenschutzrechtlichen Rechtsinn des Telemediengesetzes können Betroffene und gleichzeitig verantwortliche Stelle sein (gem. § 22 Abs. 2 und § 2 Nr. 3 TMG)

Zulässigkeit der Datenverarbeitung

- Eine Datenverarbeitung ist zulässig, wenn die betroffene Person hierin eingewilligt hat (§ 4 Abs. 1 BDSG, § 12 Abs. 1 TMG, Art. 7 Buchst. a) EU-DSRL).
- Eine **Einwilligung** ist nur wirksam, wenn dieser eine vorherige Information über die konkrete Erhebung und Verwendung von Daten vorausgegangen ist.
- Nach § 4a BDSG muss diese Erklärung auf der freien Entscheidung des Betroffenen beruhen, weshalb er auf den vorgesehenen Zweck der Verarbeitung hingewiesen werden muss. Die erteilte Einwilligung muss bestimmt sein.
- Die Einwilligung muss den konkreten Zweck, Umfang, die Art der erhobenen Daten und die daraus resultierenden Konsequenzen erkennen lassen.
- Form der Einwilligung: elektronische Form ausreichend (§ 13 Abs. 2 TMG)

Keine Einwilligung bei Facebook

- Das „Registrieren“ bei Facebook kann **nicht** mit einer datenschutzrechtlich wirksamen Einwilligung gleichgesetzt werden, weil damit keine ausdrückliche Einbeziehung des Willens der Nutzerinnen und Nutzer in sämtliche vorgesehenen und als Standard konfigurierten Formen der Datenverarbeitung erfolgt.
- Vielmehr wird lediglich pauschal auf eine Vielzahl von Dokumenten verwiesen, die durchzuarbeiten keinem Nutzer zumutbar ist.
- Facebook bietet damit den interessierten Nutzerinnen und Nutzern zwar teilweise sehr weitgehende Informationen über die durchgeführten Datenverarbeitungen. Diese Informationen sind aber nicht hinreichend bestimmt und genügen nach Ansicht des ULD **nicht** den Mindestanforderungen an Transparenz.

Problem: Social-Plugins (Like-Button)

- Binden Webseitenbetreiber Social-Plugins auf ihren Seiten ein, so initiiert Facebook beim Anklicken das Setzen des Cookies „datr“ mit einer Lebensdauer von mindestens zwei Jahren
- Gilt auch für nicht-authentifizierte und nicht-angemeldete Nutzern mit einer ID, die bei jeder Kommunikation mit Facebook oder mit dem Anklicken eines Social-Plugins wiedererkannt wird.
- Bei Facebook führt dies zu einer **Profilbildung**. Hierüber werden die Betroffenen nicht informiert.
- Auch über das gesetzlich vorgesehene Widerspruchsrecht werden sie nicht informiert. Ein solches Widerspruchsrecht mit der Möglichkeit des Ausschlusses einer Profilbildung besteht auch gar nicht.
- Die erstellten Profile werden dafür genutzt, dem jeweiligen Webseitenbetreiber Nutzungsanalysen zu ermöglichen, ihm die sog. „Insights“ zu geben.

Missachtung der E-Privacy-Richtlinie und Trennungsgebot

- Art. 5 Abs. 3 E-Privacy-Richtlinie: Setzen von Cookies, die nicht allein für die Erbringung des Dienstes erforderlich sind und genutzt werden, bedarf der Einwilligung des Nutzers.
- Nötig: Opt-in
- Diesen Anforderungen wird die Nutzung von Facebook-Social-Plugins nicht gerecht.
- § 15 Abs. 3 S. 3 TMG: „ Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden“

Analyse unangemeldeter Nutzer

- Authentifizierte/ angemeldete Nutzern: weitere Cookies, die für die Authentifizierung und die Profilbildung genutzt werden; über „datr“ kann Facebook die hierüber erlangten Nutzungsdaten einem individuellen angemeldeten Facebook-Nutzenden namentlich zuordnet.
- Nicht-authentifizierte/ angemeldete Nutzer: auch hier **Zuordnung rückwirkend möglich**, wenn die Cookie-ID binnen zwei Jahren bei einer **späteren Anmeldung** bei Facebook eindeutig zugeordnet werden kann.
- Und: Facebook erhält weitere Angaben, über die eine Identifizierung des Nutzers grundsätzlich möglich ist (IP-Adresse, Browserstring, eindeutige Webseiten-ID, Ablaufumgebung des Browsers mit Zusatzinformationen)
- Auf der Grundlage dieser Daten erfolgt auch die Reichweitenanalyse.

Ausdehnung der Nutzerkontrolle

- Der Reichweitenanalysedienst wird allen zur Verfügung gestellt, die Entwickler oder Betreiber einer Anwendung oder Seite auf der Facebook-Plattform sind.
- Facebook erstreckt damit die Erfassung der Nutzerdaten über sein eigenes Angebot **auch auf die Angebote Dritter, die Social-Plugins anbieten**
- Facebook ist somit in der Lage nachzuvollziehen, welche anderen Angebote (mit Social-Plugin) die eigenen Nutzer **außerhalb** von Facebook besuchen, wenn diese nicht aktiv eine Verfolgung über die Session Cookies durch Löschen und bewusstes Abmelden vom Netzwerk unterbinden.

Profilbildung

- Facebook als funktionaler **Auftragsdatenverarbeiter** führt für die Webseitenbetreiber und Fanpagebetreiber die Nutzungsinformationen aus der Reichweitenanalyse, die unter dem Pseudonym des Cookies erstellt werden, mit den Angaben über den angemeldeten und authentifizierten Nutzer aus dem Nutzerkonto zusammen.
- Dies verstößt gegen das gesetzliche Verbot, die erstellten Nutzerprofile dahingehend zu qualifizieren, dass sie Aussagen über die konkrete und namentlich erkennbare Person zulassen.
- Facebook ist dazu jedoch mit dem Dienst „Facebook Insights“ in der Lage und realisiert dies.

Argumente Pro Facebook

- Keine Datenverarbeitung i.S.d. BDSG bei Like-Buttons!
  - Entgegen der Ansicht des ULD hat der Betreiber einer Fanpage bei Facebook oder der Verwender des „Gefällt mir“-Button gerade **keinerlei** Kontrolle darüber welche Daten in welchem Umfang und zu welchem Zeitpunkt von Facebook erhoben werden.
  - Vielmehr sorgt die Einbindung des entsprechenden HTML-Codes lediglich dafür, dass der Internetbrowser des Nutzers eventuell eine Übertragung von Daten vornimmt. Dies ist nichts anderes als das Klicken eines Links, wobei das „Anklicken“ hier automatisiert vom Browser vorgenommen wird, wenn der Nutzer es nicht durch eine entsprechende Einstellung seines Browsers verhindert.
  - Der Fanpage-Betreiber oder derjenige, der einen „Gefällt mir“-Button einbaut erhebt aber selbst keine Daten, noch läuft die etwaige Übertragung der Daten über ihn oder seine Webseite.
- Keine Erstellung von Profilen!
  - Zwar wird die IP-Adresse übertragen eine Zuordnung geschieht aber nur dann, wenn der Nutzer auch bei Facebook registriert ist.
  - Nach Angaben von Facebook werden die IP-Adressen nach 90 Tagen gelöscht.

Argumente Pro Facebook

- Cookies und IP-Adressen nicht immer personenbezogene Daten!
  - Auslegung des Begriffs der Personenbezogenheit von Daten (§ 3 Abs. 1 BDSG) umstritten
  - Vorzugswürdig: „relative“ Betrachtungsweise plädiert. Ein und dasselbe Datum kann nach dieser Auffassung bei der einen verantwortlichen Stelle (vgl. § 3 Abs. 7 BDSG) ein personenbezogenes Datum sein und bei der anderen Stelle nicht
  - ULD: vertritt Gegenauffassung, wonach es ausreichend ist, dass es (theoretisch-abstrakt) möglich ist, das Datum mit einer natürlichen Person in Verbindung zu bringen
  - Dazu z.B. OLG Hamburg (Beschluss v. 03.11.2010, Az.: 5 W 126/10) „Dass das Ermitteln der IP-Adressen nach deutschem Datenschutzrecht rechtswidrig sein könnte, ist nicht ersichtlich, da bei den ermittelten IP-Adressen ein Personenbezug mit normalen Mitteln ohne weitere Zusatzinformationen nicht hergestellt werden kann.

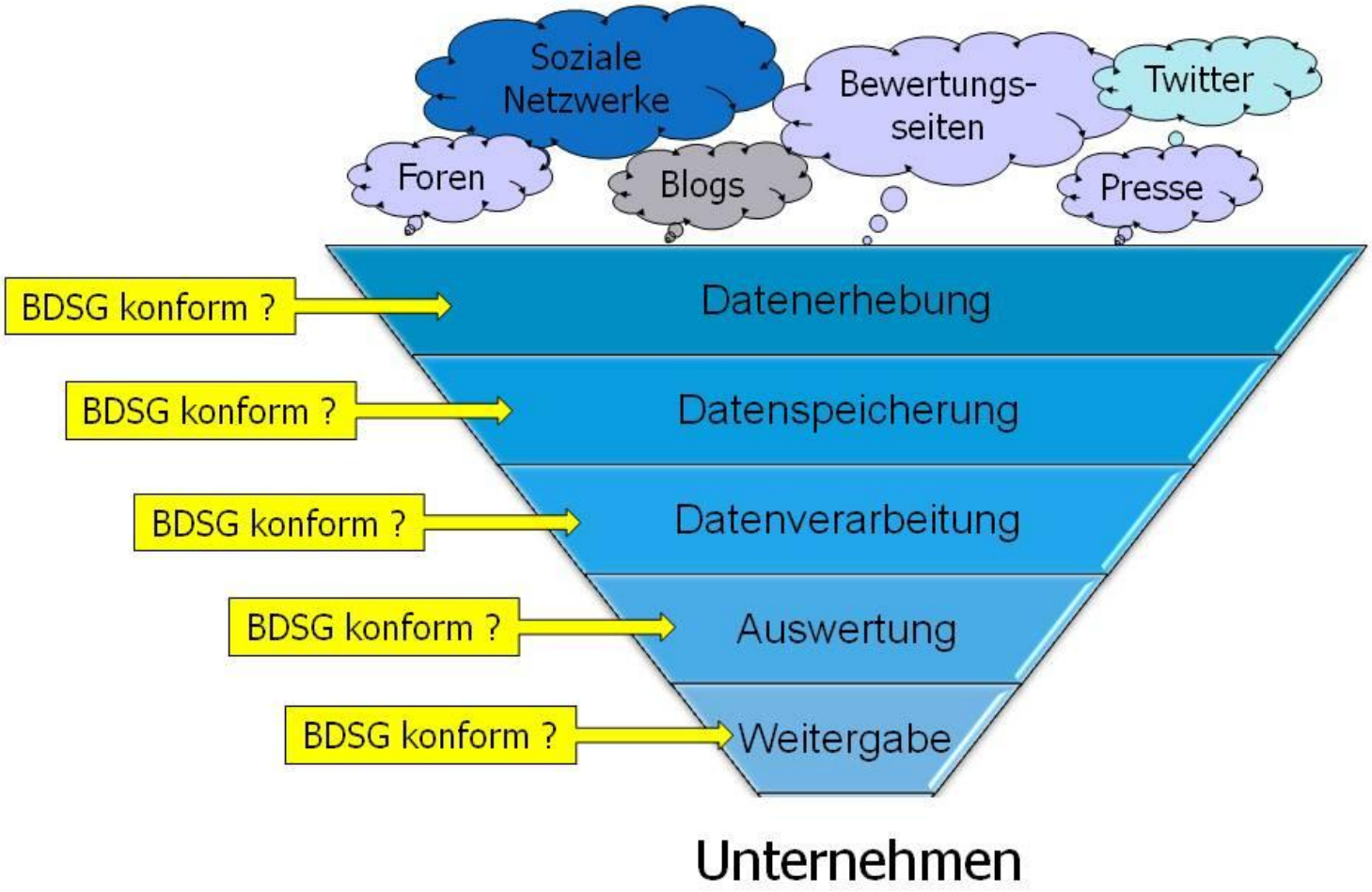
Argumente Pro Facebook

- Keine Haftung des Nutzers von Fanpage bzw. „Gefällt-mir“-Buttons als „verantwortliche Stelle“ i.S.d. § 3 Abs. 7 BDSG
  - Es ist nicht nachvollziehbar, wie das ULD auf der Grundlage der von ihm selbst beschriebenen Abläufe und dabei auch beklagten Intransparenz der Datenflüsse bzw. Nutzerinformationen im Netzwerk Facebook davon ausgehen kann, dass der Fanpage- oder Button-Verwender hier in irgendeiner Form „mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet“ oder gar „maßgeblich die inhaltlichen Entscheidungen über die Art, den Umfang und vor allem Zweck der Datenverarbeitung“ treffen kann. Es ist gerade nicht der Betreiber der Webseite bzw. der Fanpage, der die Kontrolle darüber hat, welche Daten wann und in welchem Umfang von *Facebook erhoben werden. Er hat lediglich seine Entscheidung für das „ob“ der Einbindung eines Social Plugins bzw. die Nutzung von Fanpages getroffen.*
  - Ob und ggf. in welcher Weise und in welchem Ausmaß durch Facebook eine Datenerhebung und –auswertung erfolgt, liegt nicht nur vollständig außerhalb seines Einflußbereichs, sondern tatsächlich – so ja auch das ULD – außerhalb seiner Kenntnis.
  - Seine Kontrolle beschränkt sich also darauf, das von Facebook zur Verfügung gestellte Social Plugin bzw. die Fanpage zu nutzen – oder halt nicht. Von einer irgend gearteten relevanten (Mit-)Steuerung des Prozesses der Datenverarbeitung kann daher keine Rede sein.

Argumente Pro Facebook

- keine direkte Datenerhebung und -speicherung durch den Webseitenbetreiber
  - Die Webseitenbetreiber nehmen durch die Einbindung des Like-Button-Quellcodes allenfalls eine Handlung im Vorfeld der Datenerhebung durch Facebook vor.
- Keine Inanspruchnahme der Seitenbetreiber wg. „gemeinsamer Verantwortlichkeit“ mit Facebook in Anlehnung an die Stellungnahme 2/2010 der Art. 29-Datenschutzgruppe
  - So geht die Datenschutzgruppe in vergleichbar gelagerten Fällen beim Behavioural Advertising davon aus, dass Seitenbetreiber nur eine begrenzte Verantwortung innehätten, die mit derjenigen einer verantwortlichen Stelle zwar „verwandt ist“, die ausdrücklich aber nur „eingeschränkte Datenschutz-Verpflichtungen“ mit sich bringe. Eine ähnliche Differenzierung wäre auch hier datenschutzrechtlich geboten gewesen.

Datenschutzrecht & Social Media Monitoring



Quelle: Carsten Ulbricht http://www.rechtzweinull.de/index.php?/archives/175-Social-Media-Monitoring-Datenschutz-Was-Unternehmen-beim-Durchsuchen-des-Social-Web-beachten-sollten.html

Verhaltensorientierte Werbung

- Nach Auffassung des europäischen Datenschutzbeauftragten ist „Online Behavioural Advertising“ - die Einblendung von zugeschnittenen Werbemitteln auf Websites, die sich auf eine großangelegte Beobachtung des Verbraucherverhaltens im Internet stützt - seit Überarbeitung 2009 des Artikels 5(3) der Datenschutzrichtlinie für elektronische Kommunikation nur erlaubt, wenn
  - der betreffende Nutzer nach Erhalt klarer und umfassender Informationen über die Zwecke des Tracking-Systems
  - seine Einwilligung gegeben hat,
  - in die Speicherung von Informationen wie z. B. Cookies auf seinem Computern für Tracking-Zwecke.
- http://www.edps.europa.eu

Geodaten

- Durch „Google Street View“ hat die Diskussion um die datenschutzrechtliche Bedeutung von Geodaten eine große Bedeutung bekommen.
- Weniger mit rechtlichen Argumenten (Häuserfassaden genießen kein Persönlichkeitsrecht), als mit geschicktem Schüren von Ängsten, ist es dem Datenschutzbeauftragten Hamburgs gelungen, gegenüber Google ein Recht auf Vorab-Widerspruch zu erzwingen http://www.datenschutz-hamburg.de/ihr-recht-auf-datenschutz/internet/google-street-view.html
- Einige relevante Akteure haben im März 2011 (vergeblich) versucht durch eine mit dem Wirtschaftsministerium abgestimmte Selbstverpflichtung diesbezüglich Rechtssicherheit herzustellen: http://www.bitkom.org/de/presse/8477_67099.aspx
- Nachdem dieses jedoch nicht gelungen ist, sind in Deutschland zur Zeit keine weiteren Veröffentlichungen von Bildern in Google Street View mehr geplant.

Apps für iPhone und Android

- Über die Hälfte von 1.400 untersuchten Apps (55 %) übermittelt Nutzerdaten für Zwecke der Werbung oder der Marktforschung.
- Die Einhaltung von Datenschutzbestimmungen scheint bei Apple keine besondere Rolle zu spielen.
- „What they know“ erklärt anschaulich die unterschiedlichen Datenübermittlungen von Apps http://blogs.wsj.com/wtk-mobile/
- Da diese Daten meist nicht für die eigentliche Vertragserfüllung nötig sind, bedarf dieses der Einwilligung:
- Die Einwilligungserklärung, die dem App-Nutzer dazu vorzulegen ist, muss hinreichend bestimmt sein. Dabei gilt es zwischen der persönlichen und sachlichen Reichweite zu unterscheiden.
- **Persönliche Reichweite:** Wem gegenüber willige ich ein? Welches Unternehmen erhält die Einwilligung und kann mich somit später kontaktieren?
- **Sachliche Reichweite:** Für was willige ich ein? Für welche Arten von Medien (Telefon, Fax, SMS, E-Mail) erteile ich meine Einwilligung? Für welchen Werbebereich (zum Beispiel Unterhosen, Versicherungen oder PKW) erteile ich die Einwilligung?
- Die Einwilligung muss somit alle wesentlichen Informationen enthalten, die der Nutzer zur Beurteilung dieser Umstände benötigt. Sobald hier wesentliche Informationen fehlen, wird die Erklärung unwirksam.

Recht des App-Entwicklers?

- Innerhalb der EU gilt grundsätzlich: Sitzt die Firma in einem EU-Land und erhebt von dort die Daten deutscher Nutzer, gilt das Recht des jeweiligen EU-Landes. Eine Ausnahme ist, wenn die Firma über eine inländische Niederlassung verfügt und wenn von dort die Daten erhoben werden. In diesem Fall gilt dann deutsches Recht.
- Grundsätzlich kann die Einwilligung **auch von Minderjährigen abgegeben** werden. Es kommt nicht auf das Alter der Person, sondern allein auf die Einsichtsfähigkeit des Einwilligenden an.
- Entscheidend ist bei der Beurteilung der Einsichtsfähigkeit nicht das abstrakte Alter, sondern der jeweilige geistige Entwicklungsstand des Minderjährigen sowie Art und der Umfang der erhobenen Daten.

Empfehlungen des Düsseldorfer Kreises

- **Transparenz** bezüglich der Preisgabe personenbezogener Daten: Die Nutzer müssen in die Lage versetzt werden, diese Übermittlungen nachzuvollziehen. Sie müssen auch über den jeweiligen Zweck der Datennutzungen unterrichtet werden.
- **Steuerungsmöglichkeite**n der Nutzer: Den Nutzern müssen Möglichkeiten an die Hand gegeben werden, mit denen aus der Nutzungssituation heraus gesteuert werden kann, ob und welche Daten einer Applikation zugänglich gemacht werden und an wen sie übermittelt werden.
- **Einflussmöglichkeiten** auf das Löschen von Spuren bei der Internetnutzung: Im Gegensatz zu der für herkömmliche PCs bestehenden Situation fehlt es im Smartphone-Bereich weitgehend an Möglichkeiten, Datenspuren zu vermeiden, die bei der Internetnutzung auf dem Gerät entstehen.
- Anonyme und pseudonyme **Nutzungsmöglichkeiten**: Generell sollte die Möglichkeit geschaffen werden, mit Smartphones die vermittelten Dienste anonym oder pseudonym zu nutzen.

Übermittlung von Daten Dritter

Die Welt der sozialen Medien ist eine ungerechte

- Die Übermittlung der Adressbuchdaten an Dritte (in den USA) ist **datenschutzwidrig**, da eine Einwilligung dieser Personen (soweit sie nicht selbst Nutzer des Dienstes sind) **nicht** vorliegt.
- Dienste, die nach den Regeln spielen (sowohl den gesetzlichen als auch den ethischen) und Anwendern eine maximale Entscheidungshoheit einräumen, bleibt oftmals jedoch im Markt der Erfolg versagt. Anbieter, die das Risiko in Kauf nehmen, gegen die strikten Datenschutzgesetze der EU zu verstoßen und Nutzer nur zu akzeptieren, wenn diese persönliche Informationen (Dritter) freigeben, können sich dagegen offenbar vor Mitgliedern kaum retten.
- Auf den ersten Blick erscheint dies wie ein großer Widerspruch. Auf den zweiten Blick jedoch verwundert diese Entwicklung nicht: Im Social Web siegt, wem es gelingt, das Bedürfnis der Konsumenten nach Interaktion mit ihrem Bekanntschaftskreis best- und vor allem schnellstmöglich zu befriedigen. Kenntnis über die Kontakte der Anwender ist das Rezept, um dieses Verlangen der Nutzer zu stillen, wie WhatsApp oder Viber zeigen.
- (nach: http://netzwertig.com/2011/10/27/whatsapp-kik-und-viber-datenschutz-als-bremsklotz-der-vernetzung/)

Einzelfragen: E-Mail-Marketing

- Lesetip: http://www.artegic.de/eCRM/DE/Aktuelles/Checkliste_-22-Fragen-zu-E-Mail-Marketing-und-Recht_0cq-3xm.html
  - An wen darf ich Marketing E-Mails und Newsletter versenden?
  - Wie funktioniert eine Einwilligung zum E-Mail Marketing?
  - Was muss eine Datenschutzbelehrung enthalten?
  - Welche Da ten darf ich erheben?
  - Wie lässt sich die Einwilligung des Empfängers rechtssicher nachweisen?
  - Was ist mit postalischen oder telefonischen Einwilligungen?
  - Sind Anmelde-Links für weitere Abos aus einer E-Mail heraus eine ausreichende Einwilligung?
  - Kann ich Adressen mit Opt-In kaufen und anschreiben?
  - Darf ich meine Bestands-Kontakte einmalig Anschreiben, um nach einem Opt-In zu fragen?
  - Darf ich in meinem E-Mail Marketing Werbung für Dritte – z.B. Partner oder Tochterunternehmen – verschicken?
  - Wie lange sind Einwilligungen gültig?
  - Darf man Zustimmungen zum Newsletter durch Gewinnspiele oder Rabatte fördern?
  - Wie muss eine Abmeldefunktion aussehen?
  - Muss ich von Service-E-Mails auch eine Abmeldefunktion anbieten?
  - Welche Daten darf ich aus der Analyse der Nutzung erheben?
  - Dürfen alle vorhandenen Da ten zum Kunden – auch aus verschiedenen Quellen - zusammen geführt werden
  - Muss ich Newsletter und Marketing E-Mails als Werbung kennzeichnen?
  - Muss jede E-Mail ein Impressum beinhalten?
  - Muss jede E-Mail eine alternative Textdarstellung (Multi-Part) beinhalten?
  - Darf ich in Service- und Transaktions-E-Mails werben?
  - Darf ich meinen Kontakten aus Social Networks E-Mails oder Messages schicken?
  - Darf ich die Daten meiner Kontakte aus Social Networks herunterladen und damit meine Daten anreichern?

Quellen und Hinweise

- Praxisratgeber Datenschutz und Datensicherheit, Loseblattsammlung, Mensch und Medien Verlag 2011
- „Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook“ des „Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein“ (ULD) vom 19.08.2011
- Niko Härting, „Öffentlichkeitsarbeit einer Landesbehörde Warum die ‚Facebook-Kampagne‘ des ULD verfassungswidrig ist“; http://www.computerundrecht.de/media/2011_08-22_Haerting_Oeffentlichkeitsarbeit_einer_Landesbehoerde.pdf (22.08.2011)
- Stephan Schmidt: „Verstößt die Verwendung des ‚Gefällt mir‘-Buttons wirklich gegen deutsches Datenschutzrecht?“; http://www.internet-law.de/2011/08/verstost-die-verwendung-des-%E2%80%9Egefallt-mir%E2%80%9C-buttons-wirklich-gegen-deutsches-datenschutzrecht.html (20.08.2011)
- Flemming Moos, „Dem ULD gefällt es gar nicht“; http://www.kommunikationundrecht.de/delegate/resources/ae1a273bea0b99c489a050cd236cc6ee_kur.pdf?fileid=ae1a273bea0b99c489a050cd236cc6ee_kur&type=articlepdf (K&R 10/2011)
- Jan A. Strunk, Stephan Dirks „Stellungnahme zum ‚Facebook‘-Boykott-Aufruf vom 19. August 2011 durch die schleswig-holsteinische Datenschutzbehörde ULD“; http://blawg.legalit.de/wp-content/uploads/2011/08/PM-SDP_ULD201108251.pdf (28.08.2011)
- Schleswig-Holsteinischer Landtag, Umdruck 17/2988 http://www.landtag.ltsh.de/infothek/wahl17/umdrucke/2900/umdruck-17-2988.pdf
- Cocom, Artegic Studie - http://www.artegic.de/eCRM/DE/Aktuelles/Die-Mobile-Nutzung-von-Social-Media-waechst-in-Deutschland-und-Europa-deutlich_0cq-3zn.htm
- Thomas Schwenke „Usability VS Datenschutz – Datenschutzrechtliche Einwilligung ohne Opt-In?“ http://spreerecht.de/datenschutz/2011-04/usability-vs-datenschutz-datenschutzrechtliche-einwilligung-ohne-opt-in
- Datenschutzbeauftragter „iPhone Datenschutz: Der (un)heimliche Sender“http://www.datenschutzbeauftragter-info.de/iphone-datenschutz-der-unheimliche-sender/

TAGUNG
CORPORATE MEDIA
GEZIELT. INNOVATIV. REALISIERBAR

DEUTSCHE PRESSEAKADEMIE
STUDIUM • SEMINARE • TAGUNGEN

Fragen? Fragen!

Jan Mönikes
Rechtsanwalt
www.moenikes.de
Schalast&Partner Rechtsanwälte
Dorotheenstrasse 54
10117 Berlin
jan@moenikes.de
tel: + 49 30 32 53 80 68
fax: + 49 30 32 53 80 67
mobile: + 49 172 296 75 66