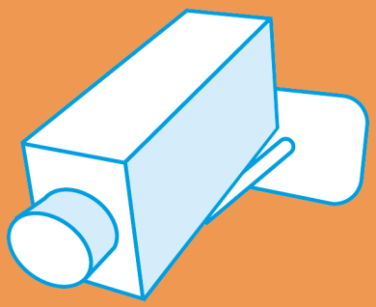
# Datenschutz
## im (mobilen) Internet



**In Kooperation von:**

internet-abc
Das Portal für Kinder, Eltern + Pädagogen

klicksafe.de
Mehr Sicherheit im Internet durch Medienkompetenz

## Impressum:

***Titel:***
Datenschutz im (mobilen) Internet (4. vollständig aktualisierte Auflage April 2015)

***Autor:***
Martin Müsgens

***Redaktion:***
Michael Schnell, Martin Müsgens

***Dank an:***
Philipp Otto und John Weitzmann, iRights.info

***Kooperationspartner und Herausgeber:***
Der Schwerpunkttext wurde in Kooperation von der EU-Initiative klicksafe – Mehr Sicherheit im Internet durch Medienkompetenz (www.klicksafe.de) und dem Projekt Internet-ABC – Das Portal für Kinder, Eltern und Pädagogen (www.internet-abc.de) veröffentlicht.

klicksafe ist das deutsche Awareness Centre im CEF Telecom Programm der Europäischen Union. klicksafe wird gemeinsam von der Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz (Koordination) und der Landesanstalt für Medien Nordrhein-Westfalen (LfM) umgesetzt. The project is co-funded by the European Union, http://ec.europa.eu/saferinternet.

Das Internet-ABC ist ein spielerisches und sicheres Angebot für den Einstieg ins Internet. Hinter dem Projekt steht der gemeinnützige Verein Internet-ABC, dem alle Landesmedienanstalten angehören. Zentrales Ziel der Vereinsarbeit ist es, Kinder und Erwachsene beim Erwerb und der Vermittlung von Internetkompetenz zu unterstützen.

***Verantwortlich im Sinne des Presserechts (ViSdP):***
Mechthild Appelhoff

***Download:***
www.klicksafe.de/materialien
www.internet-abc.de

***Kontaktadresse:***
Landesanstalt für Medien Nordrhein-Westfalen (LfM)
Zollhof 2, 40221 Düsseldorf
Tel. 0211-77007-0; Fax: 0211-727170
E-Mail: info@lfm-nrw.de
URL: www.lfm-nrw.de

Diese Onlinebroschüre steht unter der Creative-Commons-Lizenz BY-NC-ND 4.0 DE, d. h. die unveränderte, nichtkommerzielle Nutzung und Verbreitung der Inhalte auch in Auszügen ist unter Angabe der Herausgeber klicksafe und Internet-ABC sowie des Autors Martin Müsgens erlaubt. Weitere Informationen unter https://creativecommons.org/licenses/by-nc-nd/4.0/deed.de. Über die in der Lizenz genannten hinausgehende Erlaubnisse können auf Anfrage durch die Herausgeber gewährt werden. Wenden Sie sich dazu bitte an klicksafe@lfm-nrw.de oder redaktion@internet-abc.de.

## Inhalt

## 1 Einleitung


Bild: find-das-bild.de/Michael Schnell

Ob die Proteste gegen die ursprünglich für das Jahr 1983 geplante Volkszählung, Diskussionen um die Vorratsdatenspeicherung oder das Abfotografieren von Straßen und Gebäudefassaden für das Projekt Google Street View – der Schutz persönlicher Daten scheint in Deutschland ein hohes Gut zu sein. Zumindest dann, wenn die eigenen Daten von anderen erhoben und veröffentlicht werden; denn in Sozialen Netzwerken oder mobil via Smartphone geben viele Menschen weitaus privatere Sachen preis.

Zweifellos ist: Im Zeitalter von Sozialen Netzwerken, Messenger-Apps, Videoportalen, mobiler Internetnutzung und Diskussionen um eine Wiedereinführung der Vorratsdatenspeicherung stellen sich viele Fragen zum Schutz persönlicher Daten neu. Und auch wenn der ganz große Aufschrei bisher ausgeblieben ist, muss vor dem Hintergrund der Enthüllungen von Edward Snowden (Prism, Tempora, XKeyscore) vieles neu bewertet und aus einem anderen Blickwinkel betrachtet werden: Welche Auswirkungen haben die technischen Entwicklungen der letzten Jahre auf das Themenfeld Datenschutz, Schutz persönlicher Daten vor Missbrauch oder das „Recht auf informationelle Selbstbestimmung"? Wie können persönliche Daten im Zeitalter des „mobilen Mitmachnetzes" bestmöglich geschützt werden? Ist Abstinenz in Bezug auf die Einstellung eigener Inhalte und Informationen die einzig sichere Alternative, oder kann vielleicht auch ein Mittelweg gegangen werden? Und welche Rolle spielt die eigene Datensparsamkeit, wenn Freunde und Bekannte in Teilen sogar unbemerkt die eigene Person betreffende Fotos und andere intime Informationen veröffentlichen oder weiterleiten?

**Interview**

In Ergänzung zu diesem Text wurde ein Interview mit Philipp Otto und John Weitzmann von iRights.info veröffentlicht (siehe Kapitel 11). Die Experten erläutern die rechtlichen Hintergründe zum Datenschutz im Internet speziell bei Kindern und Jugendlichen und bieten zudem Informationen für Lehrkräfte und Eltern.

## 2 Datenschutz – eine (rechtliche) Annäherung

Bild: Internet-ABC

Unter dem Begriff „Datenschutz" wird umgangssprachlich zumeist der Schutz von oder der sensible Umgang mit persönlichen Daten verstanden, damit diese nicht unrechtmäßig weitergegeben oder missbraucht werden können. Juristisch ist der Begriff eng an das „Recht auf informationelle Selbstbestimmung" gekoppelt. Dieses Grundrecht wurde Ende 1983 im sogenannten „Volkszählungsurteil" konkretisiert. In den Leitsätzen zum Urteil heißt es:

1. „Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.
2. Einschränkungen dieses Rechts auf 'informationelle Selbstbestimmung' sind nur im überwiegenden Allgemeininteresse zulässig. (…)"

Auch die Europäische Menschenrechtskonvention (EMRK), an die Deutschland ebenfalls gebunden ist, macht in Artikel 8 „Recht auf Achtung des Privat- und Familienlebens" konkrete Angaben zum bürgerlichen „Recht auf Privatsphäre". Hier heißt es im Wortlaut:

1. „Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.
2. Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer."

Festzuhalten bleibt, dass persönliche bzw. personenbezogene Daten unter Berücksichtigung der oben genannten Ausnahmen in Deutschland per Gesetz vor unerlaubter Preisgabe und Verwendung geschützt sind.

Was aber sind personenbezogene Daten genau? Nach § 3 Abs. 1 des Bundesdatenschutzgesetzes (BDSG) sind personenbezogene Daten „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)". Auf der Internetseite des „Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen" werden einige Beispiele und weitere Hintergrundinformationen geliefert. Hiernach fallen unter die „Einzelangaben über persönliche oder sachliche Verhältnisse" unter anderem:

- Name, Alter, Familienstand, Geburtsdatum
- Anschrift, Telefonnummer, E-Mail Adresse
- Konto-, Kreditkartennummer
- Kraftfahrzeugnummer, Kfz-Kennzeichen
- Personalausweisnummer, Sozialversicherungsnummer
- Vorstrafen
- genetische Daten und Krankendaten
- Werturteile wie zum Beispiel Zeugnisse

**Weiterführende Links**

- Zur Volkszählung in den 1980er Jahren: www.zensus2011.de/SiteGlobals/Functions/Timeline/DE/1987/Artikel_zur_Volkszaehlung_1987.html?nn=3066692
- Gesetzestexte im Internet: www.gesetze-im-internet.de

## 3 Das Recht am eigenen Bild

Eng verknüpft mit dem „Recht auf informationelle Selbstbestimmung" ist das „Recht am eigenen Bild". In Anlehnung an die Paragraphen 22 und 23 des Kunsturheberrechtsgesetzes (KunstUrhG) gilt verkürzt, dass eine Abbildung (z. B. ein Foto) nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden darf. Hierunter fallen unter anderem die Veröffentlichung eines Fotos in einem Sozialen Netzwerk oder das Verschicken per Messenger-App (WhatsApp, Threema, etc.).


Bild: Internet-ABC

Ausschlaggebend ist die „Erkennbarkeit" der abgebildeten Person. Auf dem Bild muss also nicht unbedingt das vollständige Gesicht zu sehen sein. Es reicht, dass durch den auf dem Foto dargestellten Ausschnitt der Abgebildete eindeutig identifiziert werden kann. Wird also beispielsweise über eine abfotografierte Tätowierung auf dem Oberarm deutlich, wer auf dem Bild zu sehen ist, dann darf dieses Bild nicht ohne Zustimmung des Tätowierten veröffentlicht werden.

Folgende Ausnahmen schränken das „Recht am eigenen Bild" ein:

- Der Abgebildete ist nur „Beiwerk" und nicht der eigentliche Grund der Aufnahme. Ein klassisches Beispiel wäre, dass jemand ein Foto vom Kölner Dom macht und eine Person eher zufällig mit abgelichtet wird. Wird dieses Foto dann im Internet veröffentlicht, dann kann dieser Veröffentlichung in aller Regel nicht widersprochen werden.
- Der Abgebildete ist Teil einer Menschenansammlung, also nur „Einer von vielen". Teilnehmer von Demonstrationen oder Konzerten wären hier zu nennen.
- Der Abgebildete ist eine Person der Zeitgeschichte (z. B. ein Prominenter); aber auch Prominente müssen sich nicht jede Abbildung gefallen lassen.
- Der Abgebildete hat für die Aufnahmen ein Honorar erhalten (z. B. ein Fotomodell).
- Das Bild hat einen künstlerischen Wert und dient damit einem höheren Interesse der Kunst.

In allen anderen Fällen muss der Abgebildete vor einer Veröffentlichung oder Verbreitung gefragt werden. Eine Veröffentlichung ist es übrigens auch dann, wenn ein Foto beispielsweise in einem Sozialen Netzwerk nur einem ausgesuchten Personenkreis zugänglich gemacht wird.

Will man **Fotos von Minderjährigen** im Internet veröffentlichen oder wollen Minderjährige selbst Fotos von sich ins Netz stellen, ist in rechtlicher Hinsicht Folgendes zu beachten: Bei Kindern bis sieben Jahren sind die Erziehungsberechtigten allein entscheidungsbefugt darüber, ob eine Abbildung des Kindes veröffentlicht werden

darf. Zwischen acht und 17 Jahren hängt es vom Entwicklungsstand des jeweiligen Kindes/Jugendlichen ab: Bei entsprechendem Entwicklungsstand (Juristen sprechen hier von „erreichter Einsichtsfähigkeit") sind sowohl die Eltern/Erziehungsberechtigten als auch das Kind/der Jugendliche in die Entscheidung einzubinden (Stichwort „„Doppelzuständigkeit"). Wie Herr Weitzmann von iRights.info im Interview betont (vgl. S. 27ff.), ist rechtlich noch nicht geklärt, ob Eltern in diesen Fällen generell zustimmen müssen oder ob das Einverständnis des Jugendlichen ausreicht, solange die Erziehungsberechtigten nicht aktiv widersprechen. Von der erreichten Einsichtsfähigkeit kann in der Regel ab Vollendung des 14. Lebensjahres ausgegangen werden. Da dies in der Praxis schwer abgeschätzt werden kann, empfiehlt es sich bei nicht volljährigen Personen (z. B. im Falle der Veröffentlichung auf einer Schulhomepage), sicherheitshalber von Eltern/Erziehungs-berechtigten und der noch minderjährigen abgebildeten Person eine Einwilligung zur Veröffentlichung einzuholen – möglichst schriftlich (Vorlagen dazu siehe Link unten).

Unabhängig von der rechtlichen Situation ist es generell wünschenswert, wenn Eltern ihr Kind vorab fragen, ob es mit einer Veröffentlichung einverstanden ist.

Im Zusammenhang mit dem „Recht am eigenen Bild" ist auch Paragraph 201a „Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen" (Strafgesetzbuch StGB) von Relevanz. Dieser wurde 2014 im Nachgang an die Edathy-Affäre verändert und in Teilen verschärft. Unter anderem sind in der neuen Fassung nun auch die „Herstellung oder Übertragung einer Bildaufnahme, die die Hilflosigkeit einer anderen Person zur Schau stellt" und die „unbefugte Weitergabe einer Bildaufnahme einer anderen Person, die geeignet ist, dem Ansehen der abgebildeten Person erheblich zu schaden" strafbar.

**Weitere Informationen**

- www.gesetze-im-internet.de/stgb/ und www.gesetze-im-internet.de/kunsturhg/
- Broschüre „Nicht alles, was geht ist auch erlaubt!" und Themenreihe zu „Rechtsfragen im Netz" von klicksafe und iRights.info: www.klicksafe.de/irights
- Informationen inklusive Vorlage für entsprechende Einverständniserklärungen: www.lehrer-online.de/einwilligung-schueler.php?sid=43416342660081577239705690569430

# 4 Datenschutz im Spiegel aktueller Trends und Entwicklungen

Auch wenn eine gewisse Sensibilität im Umgang mit persönlichen Daten bereits vor dem digitalen Zeitalter wichtig war, haben Internet, Smartphones und weitere technische Entwicklungen den Stellenwert dieses Themas stark vergrößert. Um sich dies bewusst zu machen, kann einmal der Versuch unternommen werden, nur einen Tag beim Surfen im Internet keine persönlichen Daten von sich preiszugeben und zudem keinen Dienst zu nutzen, der auf persönliche Daten zugreift (IP-Adresse ausgenommen). So bekommt man schnell eine Vorstellung davon, wie häufig personenbezogene Daten im Internet abgefragt, genutzt und weitergegeben werden – vielfach auch unbemerkt im Hintergrund. Bei der Nutzung eines Smartphones ist ein solches Unterfangen von vorne herein zum Scheitern verurteilt.

Bedenkt man dann noch, dass persönliche Daten und Fotos auch von anderen Nutzern eingestellt werden, wird das Ausmaß noch deutlicher. Die in diesem Zusammenhang wesentlichen Entwicklungen werden nachfolgend vorgestellt.

## 4.1 Das Social Web oder der Weg zum „Mitmachnetz"

Noch bis in die Anfangsjahre dieses Jahrtausends war das Internet für die meisten Nutzer vor allem eine informationelle Einbahnstraße. Mit nach heutigen Standards geringen Verbindungsgeschwindigkeiten – der eine oder andere mag sich noch an den Einwahlton des 56k-Modems erinnern – rief man von anderen eingestellte Informationen ab. So war der überwiegende Teil der Internetnutzer ausschließlich Konsument und nutzte das Internet ähnlich wie Fernsehen, Zeitung oder Radio rezeptiv.

Dies änderte sich vor allem durch das Aufkommen der Sozialen Netzwerke wie Facebook oder studiVZ ab ungefähr 2003-2004. Aber auch Video- und Bildportale oder das (häufig illegale) Tauschen von Musik-, Bild- und Filmdateien über Tauschbörsen oder Filehoster führten dazu, dass die Nutzer selbst zunehmend eigene Inhalte erstellten und diese im Internet veröffentlichten. Eine wesentliche Voraussetzung schuf die zunehmende Verbreitung von schnellen Breitbandanschlüssen, die ein komfortables Hochladen von Bild- und Videodateien erst ermöglichten. Das Mitmachnetz „Web 2.0" war geboren.

Heute hat der sogenannte „User-Generated Content" (also von den Nutzern des Internets hochgeladene Inhalte) bereits extreme Ausmaße erreicht – Tendenz steigend. So werden beim Videoportal YouTube pro Minute weltweit im Schnitt ca. 72 Stunden neues Filmmaterial hochgeladen. Im Sozialen Netzwerk Facebook werden im gleichen Zeitraum weltweit durchschnittlich 100.000 Freundschaftsanfragen gestellt (Quelle siehe „Weitere Informationen"). Soziale Netzwerke sollen aufgrund ihrer aktuell noch recht hohen Bedeutung und Verbreitung im Folgenden gesondert vorgestellt werden.

**Weitere Informationen**

- Was in 60 Sekunden im Internet passiert (inklusive Infografik): www.faz.net/aktuell/wirtschaft/wirtschaft-in-zahlen/grafik-des-tages-was-binnen-einer-minute-im-internet-passiert-13459083.html

## 4.2 Soziale Netzwerke – Facebook und Co.

Soziale Netzwerke (auch Social Communities genannt) haben einen nahezu unvergleichbaren Siegeszug vorzuweisen. Allein das aktuell bekannteste und gleichzeitig erfolgreichste Netzwerk Facebook kommt nach eigenen Angaben weltweit auf knapp 1,39 Milliarden aktive Nutzer pro Monat und wird in knapp 50 Sprachen angeboten. In Deutschland hat Facebook ca. 26 Millionen Nutzer – zunehmend auch mobil. War bei den jüngeren Nutzern vor ein paar Jahren primär das im Mai 2013 eingestellte deutsche Netzwerk schülerVZ angesagt, so hat sich auch hier Facebook inzwischen durchgesetzt (siehe z. B. KIM-Studie 2014, S. 37ff.). Auch das deutsche Angebot wer-kennt-wen musste im Juni 2014 dem Konkurrenzdruck nachgeben und sein Angebot schließen. Als Konsequenz verlassen nun auch die Daten dieser Altersgruppe immer häufiger die Landesgrenzen, da sämtliche auf Facebook eingestellten Informationen auf Servern in den USA gespeichert werden. Obwohl Facebook nach den AGB erst ab 13 Jahren ist, ermittelte die KIM-Studie ein Durchschnittsalter von 10,4 Jahren bei der ersten Anmeldung in einer Community.

In der Presse wird immer wieder das Ende bzw. eine Überalterung von Facebook ausgerufen (vgl. zum Beispiel sueddeutsche.de oder tagesspiegel.de). Und tatsächlich hat die JIM-Studie 2014 (S. 35 ff.) gezeigt, dass bei den 12-19-Jährigen seit 2013 ein deutlicher Rückgang von 80 auf 69 Prozent (2014) bei der Facebook-Nutzung zu verzeichnen ist. In Teilen kann dies mit einer Verlagerung auf andere Dienste (Messenger Apps wie WhatsApp oder Angebote wie Instagram oder Tumblr) erklärt werden. Trotzdem liegt Facebook in 2014 bei den Jugendlichen noch klar vorne. Es bleibt abzuwarten, ob dieser Abwärtstrend anhält. Facebook sorgt hier in jedem Fall schon einmal vor, was die Aufkäufe von Instagram 2012 und WhatsApp Anfang 2014 belegen.

Die Frage, ob man sich ein Profil in einem Sozialen Netzwerk zulegen will oder nicht, muss jeder für sich selbst beantworten. In jedem Fall gilt: Will man sinnvoll bei Sozialen Netzwerken mitmachen, ist es unerlässlich, persönliche Daten zu veröffentlichen. Schließlich will man in aller Regel ja von anderen Nutzern gefunden werden. Der richtige Spagat zwischen Privatsphäre und Öffentlichkeit ist nicht immer leicht – für Jugendliche und Erwachsene gleichermaßen.

Warum sollte man sich aber überhaupt über die eingestellten Daten Gedanken machen? Schließlich erfahren (bei entsprechend sensiblen Privatsphäre-Einstellungen) ja nur Freunde und Bekannte oder sogar nur gesondert ausgewählte Personen davon. Da aber auch die Anbieter Sozialer Netzwerke „mitlesen", ist ein genauerer Blick auf die Geschäftsmodelle Sozialer Netzwerke notwendig.

**Geschäftsmodelle Sozialer Netzwerke**

Die Mitgliedschaft in Sozialen Netzwerken ist in der Regel umsonst. Warum haben große, nach Wirtschaftlichkeit strebende Unternehmen ein Interesse daran, den Verbrauchern mit viel Aufwand einen Gratisdienst anzubieten? Der einfache Grund: Die Nutzer zahlen mit den eingestellten persönlichen Daten und Informationen. Diese werden vom jeweiligen Anbieter ausgewertet und mit anderen Informationen verknüpft, um den Nutzern beispielsweise an den jeweiligen Interessen ausgerichtete Werbebanner zu zeigen. Man spricht hier von „personenbezogener Werbung".

Zudem werden die Daten (nach Unternehmensangaben in anonymisierter Form) auch an andere Firmen weitergeleitet. Im Grunde gilt, dass Kundendaten, Kaufgewohnheiten, Interessen und weitere Informationen früher noch aufwendig über Fragebögen erhoben werden mussten. Heute liefern die Mitglieder von Sozialen Netzwerken und anderen Diensten diese Daten bereitwillig selbst und geben dabei vielfach mehr von sich preis, als sie es in den klassischen Verbraucherbefragungen je tun würden.

Um sich genauer darüber zu informieren, auf welche Daten der Anbieter zugreift und was er mit den Informationen genau macht, empfiehlt es sich, die Allgemeinen Geschäftsbedingungen des Angebots (AGB) und die darin enthaltenen Datenschutzrichtlinien genau zu studieren – möglichst vor der ersten Anmeldung. Da diese nicht in Stein gemeißelt sind und sich laufend ändern, ist es sinnvoll, hier regelmäßig nachzuprüfen. Um eine Vorstellung davon zu bekommen, welche Daten Facebook (je nach Art der verwendeten Dienste) sammelt, hilft ein Blick in die aktuellen Datenschutzrichtlinien von Facebook. Dort sind aktuell folgende Punkte gelistet:

- Deine Aktivitäten und von dir bereitgestellte Informationen.
- Die Aktivitäten anderer und von ihnen bereitgestellte Informationen.
- Deine Netzwerke und Verbindungen.
- Informationen zu Zahlungen.
- Geräteinformationen.
- Informationen von Webseiten und Apps, die unsere Dienste nutzen.
- Informationen von Drittpartnern.
- Informationen von anderen Facebook-Unternehmen.

**Vorsicht: Daten können außer Kontrolle geraten!**

Nicht nur für Soziale Netzwerke, sondern für das Internet generell gilt, dass veröffentlichte oder versendete Daten leicht eine Art „Eigenleben" entwickeln können und die Verbreitung so außer Kontrolle gerät. Jedes eingestellte oder versendete Bild, jede gepostete Information kann von anderen Nutzern (oder dem jeweiligen Anbieter des Dienstes) kopiert und gespeichert werden und so immer wieder im Netz auftauchen – also auch Jahre später, lange nachdem sie von der Ursprungsstelle entfernt worden ist. Hierdurch werden die Daten zudem aus dem ursprünglichen Kontext gelöst, wodurch die eigentliche Intention und Bedeutung verfälscht und verfremdet werden können.

Auch aus diesem Grunde ist es sinnvoll, sich gleich bei der Registrierung mit den Privatsphäre-Einstellungen des Netzwerkes vertraut zu machen. Da die Funktionalitäten von Sozialen Netzwerken laufend erweitert werden, sollte man diese Einstellungen zudem regelmäßig auf Passung prüfen. Ebenfalls ist es empfehlenswert sich genau anzuschauen, welchen Kontakten man Zugriff auf bestimmte eher private Informationen gewähren möchte. Und unabhängig vom Alter sollten sich auch Erwachsene Nutzer von Sozialen Netzwerken vor dem Hochladen von Fotos und anderen Informationen immer mal wieder die Frage stellen, wie die jeweilige Info bei anderen Nutzern ankommt und ob diese ggf. auch missverstanden oder missbraucht werden könnte.

Darüber hinaus werden in vielen Fällen auch die eigene Person (oder die eigene Familie) betreffende Daten von anderen Personen hochgeladen. In diesem Zusammenhang war es ein wichtiges Ergebnis der LfM-Studie „Heranwachsende und Datenschutz auf Sozialen Netzwerkplattformen", dass viele Jugendliche vergleichsweise sensibel sind, wenn es um die nicht autorisierte Veröffentlichung sie selbst betreffender Daten durch andere geht. Auf der anderen Seite liegt aber häufig nur ein geringes Problembewusstsein bezüglich der nicht abgestimmten Einstellung von Daten anderer Nutzer vor (siehe Link unten).

Zudem zeigte der Skandal rund um Prism, Tempora und die NSA, dass neben dem Anbieter selbst auch staatliche Stellen genauer hinschauen, als viele Internetnutzer und –nutzerinnen für möglich gehalten haben. Dies können auch noch so strenge Privatsphäre-Einstellungen nicht verhindern. Hier ist Datensparsamkeit in vielerlei Hinsicht die einzig wirklich sichere Alternative.

**Weitere Informationen**

- Landesanstalt für Medien Nordrhein-Westfalen (LfM) (Hrsg.): Heranwachsen mit dem Social Web, 2., unver. Aufl. 2011: www.lfm-nrw.de/forschung/schriftenreihe-medienforschung/band-62.html
- Infos zu Facebook, Tumblr, Instagram, ask.fm und Datenschutz in Sozialen Netzwerken: www.klicksafe.de/themen/kommunizieren/soziale-netzwerke und www.klicksafe.de/facebook

- Wissen, wie's geht: Soziale Netzwerke: www.internet-abc.de/eltern/online-communitys.php

## 4.3 Mobil ins Internet und standortbezogene Dienste

Bild: find-das-bild.de

Eine weitere Entwicklung, die sich deutlich auf datenschutzrechtliche Fragestellungen ausgewirkt hat, ist die mobile Internetnutzung über Smartphone, Tablet und andere portable Geräte. Vor allem fallende Preise für mobiles Internet haben dazu geführt, dass inzwischen 86 Prozent der befragten 12- bis 19-jährigen Jugendlichen auch mobil über Handy/Smartphone ins Internet gehen; 2012 fiel der Anteil mit 49 Prozent deutlich niedriger aus (vgl. auch JIM-Studie 2014, S. 24 ff.).

Surfen die meisten Nutzer daheim noch mit (relativ) abgesicherten Computern oder Laptops (Virenprogramm, WLAN-Verschlüsselung, Firewall, Anti-Spyware-Programme), wird quasi „zur Wiedergutmachung" über die aktuell noch relativ ungesicherten Mobilfunk- oder WLAN-Netze in Cafés, Hotels, Flughäfen, etc. fröhlich Home-Banking oder Onlineshopping betrieben. Dass „erwachsene" Nutzer hierbei vorsichtiger wären als jugendliche Mobil-Surfer, soll zumindest in Frage gestellt werden. Die Bequemlichkeit lässt datenschutzrechtliche Problemstellungen offenbar vielfach nebensächlich erscheinen.

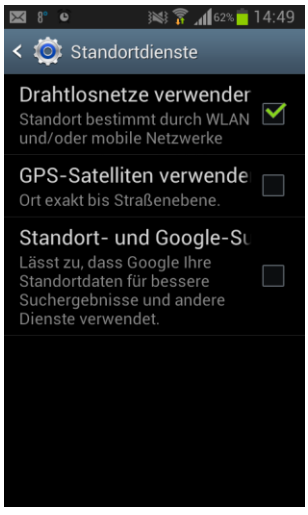



Bild: Android 4.1.2, 30.03.2015

Immer häufiger wird bei der Handynutzung über GPS, WLAN oder mobile Netzwerke automatisiert auch der aktuelle Standort des Nutzers abgefragt. So können Unternehmen beispielsweise auf passende (kommerzielle) Angebote im näheren Umkreis verweisen oder entsprechende Apps können dem Nutzer mitteilen, welche Freunde oder Bekannte sich gerade in der Nähe aufhalten. Ist die permanente Erfassung und Weitergabe des Standorts nicht deaktiviert (siehe Screenshot rechts), können Unternehmen regelrechte Bewegungsprofile ihrer Kunden erstellen. Standortbezogene Dienste werden in Zukunft

immer wichtiger und zunehmend ausgebaut – und damit ist auch der eigene Standort ein schützenswertes Gut!

**Weitere Informationen**

- Themenreihe von klicksafe und iRights.info: www.klicksafe.de/irights
  - Text 27: Geo-Location: Das Wo im Netz und
  - Text 31: Vom Web-Tracking zum App-Tracking
- Handysektor: Datenschutz – Das einfache Spiel der Datensammler: www.handysektor.de/datenschutz-recht/datenschutz.html
- ZEIT ONLINE: Bewegungsprofile sind individueller als gedacht: www.zeit.de/digital/datenschutz/2013-04/bewegungsprofil-forscher-zuordnung

## 4.4 Apps – Apps – Apps

Apps haben auf Smartphones und Tablets eine unglaubliche Erfolgsgeschichte hinter sich. Die Zahl der am Markt erhältlichen Apps hat die Millionengrenze längst überschritten. Allein die Zahl der in Apples App-Store eingestellten Apps erhöhte sich von 500 im Juli 2008 auf über 1,2 Millionen (Stand: Juni 2014, inkl. Apps von Drittanbietern; Zahlen nach Wikipedia, Art. App-Store (iOS)).

Was aber ist eine App und was haben Apps mit dem Thema Datenschutz gemein? „App" ist die Kurzform von Application, also Anwendung oder Programm. Apps können je nach Betriebssystem über verschiedene App-Stores oder in Teilen auch über inoffizielle Webseiten entweder kostenlos oder gegen Gebühr heruntergeladen und installiert werden. Durch Klick auf ein kleines Symbol werden diese Programme nach der Installation gestartet. Apps können kleine Spiele sein, Nachrichten aus aller Welt präsentieren, die Fahrpläne für Busse und Bahnen angeben oder auch gänzliche „Quatschanwendungen" (Nacktscanner, Röntgengeräte, virtuelle Feuerzeuge, Gedanken lesende Apps, etc.) sein. Es gibt immer wieder Apps, die besonders angesagt sind und die man einfach haben muss. Beliebt sind v. a. Apps, die der Kommunikation und Vernetzung dienen, wie z. B. WhatsApp oder die Apps Sozialer Netzwerke wie Facebook. Gerade bei Kindern und Jugendlichen kann der Gruppenzwang zur Installation hier sehr hoch sein.

**Apps in Sozialen Netzwerken**

Seit ca. 2007 fühlen sich Apps auch in Sozialen Netzwerken überaus wohl. Diese werden innerhalb des eigenen Sozialen Netzwerkprofils „installiert" und aufgerufen. Sie sind mit der Oberfläche des Sozialen Netzwerks fest verwoben. Freunde und Bekannte werden (so nicht in den Einstellungen des Netzwerks deaktiviert) darüber informiert, welche Apps man gerade nutzt. Auch das Erreichen bestimmter Erfolge (hohe Punktzahlen, Level, etc.) wird bei vielen Spiele-Apps an den virtuellen Freundeskreis kommuniziert. Apps in Sozialen Netzwerken sind in der Grundversion in aller Regel gratis. Will man schneller zum Erfolg kommen, können häufig gegen Gebühr virtuelle Vorteile erworben werden (z. B. eine bessere Rüstung, ein leistungsfähigerer Traktor oder Ähnliches).

**Apps – Bezahlen mit Daten**

Das Geschäftsmodell vieler vor allem kostenloser Apps entspricht dem vorgestellten Modell Sozialer Netzwerke, und so bedeutet auch hier gratis in vielen Fällen nicht kostenlos. Vielmehr zahlt man indirekt über die Bereitstellung bestimmter Daten oder Funktionen, auf die die App zugreift. Eine Ausnahme ist hierbei die Unternehmensstrategie, Apps zunächst kostenlos und sie erst dann gegen Gebühr anzubieten, wenn sie eine bestimmte Verbreitung oder Bekanntheit erreicht haben und ein Verzicht entsprechend schwerer fällt.

Wie gelangt eine App aber an diese Daten? Viele Apps fordern gewisse Berechtigungen ein, zum Beispiel ein Zugriff auf den aktuellen Standort, die Kontakte, den Kalender oder die Kamera. Welche Daten dies genau sind, wird beim Betriebssystem Android bereits vor der Installation angezeigt (siehe Abbildung rechts). Beim iPhone (iOS) müssen die Berechtigungen zwar vor der Installation nicht vom Nutzer akzeptiert werden, können aber – anders als bei Android – im Nachhinein in Teilen wieder zurückgenommen werden (siehe „Weitere Informationen" unten). Bei Android heißt es in der Regel „Friss oder stirb", oder schöner formuliert: Entweder man akzeptiert die eingeforderten Berechtigungen, oder man kann die App nicht nutzen. Lediglich über die Installation

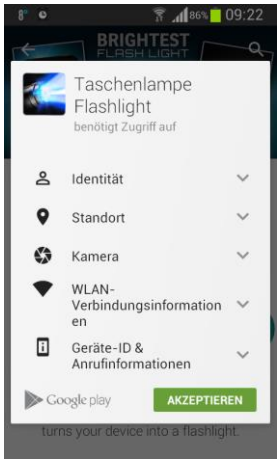



Bild: Screenshot Google Play Store, 20.03.2015

spezieller Apps von Drittanbietern können einzelne Berechtigungen in Teilen zurückgenommen werden.

Wichtig ist zu betonen, dass eine App, die viele Berechtigungen einfordert deshalb nicht unbedingt schlecht oder unseriös sein muss (siehe auch „Weitere Informationen"). Zum Beispiel kann keine Navigations-App ohne Zugriff auf den aktuellen Standort funktionieren. Will eine Navigations-App Zugriff auf die gespeicherten Kontakte haben, kann dies auch bedeuteten, dass die App auch die Funktion enthält, sich die Route zu gespeicherten Kontakten anzeigen zu lassen (siehe auch Abschnitt „Keine Panik!"). So gilt es vielmehr zu prüfen, ob die eingeforderten Berechtigungen im Sinne des Funktionsumfangs notwendig sind oder nicht. Die Wahrscheinlichkeit, dass eigentlich nicht benötigte Berechtigungen eingefordert werden, ist bei kostenlosen Apps im Sinne des zugrunde liegenden Geschäftsmodells höher.

Darüber hinaus gibt es bei Apps weitere Finanzierungsmodelle. Einige Apps funktionieren nach dem Freemium-Prinzip (Kunstwort aus Free und Premium). Hier gibt es eine im Funktionsumfang begrenzte kostenlose Version, die Lust auf mehr machen soll. Die Version mit allen Funktionen ist dann nur gegen Gebühr zu haben. Manchmal enthält die freie Version auch Werbeeinblendungen und erfordert mehr Berechtigungen als die kostenpflichtige Version. Bei anderen Apps können „aus der App heraus" bestimmte zusätzliche Leistungen oder Vorteile eingekauft werden, z. B. um in Spielen besondere Gegenstände zu erwerben. Gerade jüngeren Kindern ist hierbei nicht immer klar, dass tatsächliche Kosten entstehen. Eltern sollten In-App-Käufe so möglich sicherheitshalber mit einem Passwort schützen (siehe „Weitere Informationen").

Im Zusammenhang mit Apps stellt sich zudem die Frage, ob AGB und Datenschutzrichtlinien eines Angebots variieren, je nachdem, ob man einen Dienst über einen Internetbrowser oder über eine App aufruft. Weiterhin gilt es zu prüfen, ob die gewählten Datenschutzeinstellungen beispielsweise eines Sozialen Netzwerks auch dann noch vollständig aktiv sind, wenn das Netzwerk über ein App gestartet wird. Hier kann ein Vergleich der AGB, Datenschutzrichtlinien und -einstellungen nicht schaden.

**Keine Panik!**

Trotz der genannten Einschränkungen ist auch im Zusammenhang mit Apps vor übertriebener Panik zu warnen. Viele Apps sind sehr praktisch und erleichtern den Alltag. Man sollte vor einer Installation aber genau hinsehen, welche Nutzungsbedingungen und Datenschutzrichtlinien der App zugrunde liegen und auf welche Informationen die App zugreift (siehe „Der App-Check"). Auch die Seriosität des Anbieters sollte man sich vor einer Installation anschauen, beispielsweise indem man die Wertungen anderer Nutzer ansieht oder auf der Seite des Anbieters prüft, wer genau hinter dem Angebot steht. Apps sollten zudem möglichst nur von den offiziellen App-Stores bezogen werden. Bevor man eine App aktualisiert, sollte generell gegengeprüft werden, ob mit der Aktualisierung eine Erweiterung der Zugriffsrechte einhergeht. Aus diesem Grunde ist es empfehlenswert, Apps vom System nicht automatisiert aktualisieren zu lassen.

**Weitere Informationen**


- klicksafe-Bereich zum Thema Smartphone und Apps: www.klicksafe.de/smartphones und www.klicksafe.de/apps
- Broschüre „Smart mobil?!" von klicksafe und Handysektor: www.klicksafe.de/materialien
- Anleitungen zum Passwortschutz von In-App-Käufen bei Android und iOS: www.klicksafe.de/themen/kommunizieren/smartphones/apps-abzocke/
- www.klicksafe.de/irights:
  - Text 31: Vom Web-Tracking zum App-Tracking
  - Text 33: Handys an Schulen
  - Text 34: „Was sollte ich beim Kauf von Apps beachten?"
- Handysektor – Infos zu Apps, Berechtigungen, Smartphones, Tablets und mobilen Netzen: www.handysektor.de
- Frankfurter Allgemeine: Apps – Ausgespäht vom eigenen Smartphone: www.faz.net/aktuell/technik-motor/computer-internet/apps-ausgespaeht-vom-eigenen-smartphone-12282473.html

## 4.5 Onlinebanking, Onlineshopping und Onlinebooking

Bild: find-das-bild.de/Redaktion

Zeitmangel, Bequemlichkeit und häufig günstigere Angebote führten dazu, dass sich bei vielen Nutzern ihre Bankgeschäfte und ein zunehmender Anteil ihrer Einkäufe auf das Internet verlagert haben. Fernseher, Katzenfutter, Flüge, Konzerte, Hotelreservierungen – nichts, was man nicht auch bequem von der eigenen Couch aus bestellen oder buchen könnte. Hierbei müssen dem Anbieter zwangsweise viele persönliche Daten mitgeteilt werden: Die vollständige Adresse ist im Grunde immer notwendig, die bestellte Ware soll ja ankommen. Da man die Ware auch bezahlen muss, werden in der Regel Bank- oder Kreditkartendaten abgefragt. Eine Telefonnummer für Rückfragen und die E-Mail-Adresse für die Registrierung sind den meisten Onlineshopping und Onlinebooking-Portalen ebenfalls bekannt.

Überlegt man sich einmal, welches Wissen Onlineversandhändler über die Zeit und mit jeder Bestellung über ihre Kunden erlangen, ist es zum gläsernen Konsumenten häufig nicht mehr weit: Hobbys, Familienstand, Kinder oder kinderlos, Interessen – all dies kann relativ leicht aus den getätigten Einkäufen abgeleitet werden.
Im Zuge der Zeit kann zudem leicht der Überblick darüber verloren gehen, welchen Firmen man Bank- und Adressdaten, Geburtsdatum, E-Mail-Adresse und andere Daten anvertraut hat. Dies muss nicht zum Problem werden, aber es kann.

### Weitere Informationen

- Verbraucherzentrale NRW: Datenschutz beim Onlinebanking: www.vz-nrw.de/datenschutz-beim-online-banking

## 4.6 Der Trend zur Cloud oder „Ab in die Wolke"

Bild: find-das-bild.de/Montage Internet-ABC

Ein weiterer Trend der Zeit ist es, Daten nicht mehr nur auf dem eigenen Computer zu speichern, sondern sie „in die Cloud auszulagern". Die Cloud (wörtlich „Wolke") ist hierbei im Grunde nichts anderes als externer Speicherplatz im Internet. Diesen Speicherplatz kann man nun mit ei-

genen Dokumenten, Fotos usw. befüllen und von allen Orten und Computern auf diese Daten zugreifen. Ein solcher Service kann sehr praktisch sein, z. B. wenn man die Urlaubsbilder bereits im Urlaub zur Sicherheit auch in die Cloud ablegt. Bei vielen aktuellen Betriebssystemen ist die Cloud-Anbindung so tief im System verankert, dass es schon eines gewissen Know-hows bedarf, die teilweise sogar automatische Speicherung von Dokumenten, Texten und anderen Dateien in der Cloud zu unterbinden. Die hochgeladenen Daten können mit einem Passwort gegen unberechtigte Zugriffe gesichert werden. Je nach Anbieter kann der Zugriff auf Dateien auch einzelnen Nutzern oder über einen öffentlichen Link allen Interessierten gewährt werden. Zunehmend werden auch Programme in die Cloud abgelegt, um diese von verschiedenen Rechnern aus starten zu können.

Die Speicherung persönlicher Dateien auf externen Servern ist immer mit dem Risiko verbunden, dass sie von unberechtigten Personen eingesehen werden. Zudem sitzen viele Anbieter im Ausland, weshalb die eigenen Daten schon beim Speichern die Landesgrenzen verlassen. Dies muss nicht, kann aber aufgrund unterschiedlicher Gesetzgebung im Land des Anbieters nachteilig sein. Auch gilt nachzufragen, was mit den Daten passiert, wenn ein Anbieter seinen Dienst aufgibt oder in Konkurs geht.

**Weitere Informationen**

- iRights.info Dossier „Speichern in der Cloud“: http://irights.info/dossier/cloudspeicher
- Internet-ABC: Cloud Computing – Was ist los in der Datenwolke?: www.internet-abc.de/eltern/cloud-computing-datenwolke.php

## 5 Warum Datenschutz uns alle angeht (und zunehmend wichtiger wird)

Alle im Internet eingestellten oder über das Internet übertragenen Informationen können abgefangen oder missbraucht werden. Bei Bank- und Kreditkartendaten wäre dies besonders schmerzhaft. Ebenfalls unerwünscht dürfte in den meisten Fällen eine für alle sichtbare Einstellung der Privatadresse oder der eigenen Handy- oder

Festnetznummer im Internet sein. Nervende Werbeanfragen wären hier unter harmlosere Folgen zu fassen. Und obwohl es bereits erste Verfahren gibt, Dateien, wie 2011 von der damaligen Verbraucherschutzministerin Aigner gefordert, mit einem Verfallsdatum zu versehen, wird es einen wirksamen „virtuellen Radiergummi", der beispielsweise auch bei von anderen Nutzern eingestellten persönlichen Inhalten greift, wohl in absehbarer Zeit nicht geben.

Bild: find-das-bild.de/Montage Internet-ABC

Hierbei ist zudem von Bedeutung, dass bei einem Versand über Apps die Inhalte nicht mehr „nur" auf dem Server des Anbieters liegen, sondern diese zusätzlich auf allen angeschriebenen Geräten gespeichert werden; ein Löschen ist so noch schwieriger geworden (vgl. auch Kapitel 9). Aber auch gegen unberechtigte Zugriffe besonders gesicherte Daten (z. B. über eine Verschlüsselung des betrieblichen oder privaten E-Mail-Verkehrs) können in falsche Hände geraten. Spektakuläre Hacking-Attacken, bei denen auf einen Schlag Kunden- und Kreditkartendaten von Tausenden oder sogar von mehreren Millionen Nutzern illegal heruntergeladen werden, zeigen, dass auch große Unternehmen nicht davor geschützt sind (vgl. auch den Hackerangriff auf private Prominentenfotos in 2014).

Warum aber ist es so leicht, im Internet an Informationen beispielsweise über eine bestimmte Person zu kommen? Ein Vorteil des Internets ist gleichzeitig ein Grundproblem in Sachen Datenschutz: das Internet kann sehr komfortabel nach ausgewählten Inhalten durchforstet werden – vielfach sogar automatisiert. Und so können auch Daten, die für sich genommen eher weniger delikat sind, in Verknüpfung mit anderen Informationen ein immer genaueres Bild der eigenen Person liefern. Denn im Grunde ist jedes veröffentlichte Datum, jede kleinste Information ein kleines Puzzlestück der eigenen Persönlichkeit. Hinzu kommt die bereits vorgestellte Möglichkeit, Daten mit nur einem Mausklick zu kopieren um diese systematisch im Internet zu streuen und so die Langlebigkeit im Internet bestmöglich zu unterstützen. Wer eine eigene Homepage besitzt oder vor Jahren einmal besessen hat, dem sei in Sachen „Langzeitgedächtnis des Internets" ein Besuch bei www.archive.org empfohlen. Hier kann mittels WayBackMachine eine virtuelle Zeitreise unternommen werden und der Stand einer beliebigen Internetseite zu unterschiedlichen Zeitpunkten abgerufen werden.

Welche Informationen über die eigene Person bereits im Internet kursieren und wie leicht es ist, diese kompakt zu verknüpfen, kann neben den klassischen Suchmaschinen auch über spezielle Personensuchmaschinen wie www.yasni.de laienhaft nachvollzogen werden. Große Unternehmen oder staatliche Einrichtungen haben hier noch ganz andere Möglichkeiten.

**Weitere Informationen**

- SPIEGEL ONLINE: NSA-Programm Prism – Alle Artikel und Hintergründe www.spiegel.de/thema/nsa_programm_prism
- ZEIT ONLINE: Verschlüsselung – Die halbsichere „E-Mail made in Germany" www.zeit.de/digital/datenschutz/2013-08/email-telekom-gmx-verschluesselt

## 6 Exkurs: Abzocke im Netz – Preisausschreiben, Gratisklingeltöne, Hausaufgabenhilfe

Vielfach stößt man im Internet auch auf Angebote von nicht immer seriösen Anbietern, die Intelligenztests, Software, Hausaufgabenhilfen, Preisausschreiben mit lukrativen Gewinnen oder auch die neuesten Klingeltöne aus den Charts anbieten. Bereits im zweiten Schritt werden dann sehr detaillierte Nutzerdaten abgefragt. Hierbei sollte man generell sehr vorsichtig sein und genau hinschauen. Denn häufig sind Hinweise auf tatsächlich anfallende Kosten gut versteckt angebracht, und einige Zeit später liegt eine Rechnung im Briefkasten. Seit August 2012 wird Internetabzocke durch die „Button-Lösung" erschwert; nach dieser gesetzlichen Regelung müssen Verbraucher auf entstehende Kosten per eindeutig beschriftetem Button hingewiesen werden. Ansonsten kommt kein kostenpflichtiger Vertrag zustande.
Fällt man selbst oder ein Familienangehöriger auf eine Abzockfalle herein, sind die Verbraucherzentralen die passenden Ansprechpartner. Auf den Aspekt „Abzocke im Internet" im Detail einzugehen, würde den Rahmen dieses Artikels sprengen. Informationen findet man beispielsweise auf folgenden Webseiten:

- Internet-ABC: Schwerpunkt „Abzocke und Kostenfallen" www.internet-abc.de/eltern/abzocke-kostenfallen-abonnements.php
- checked4you: Onlineabzocke: www.checked4you.de/abzocke

- Text „Onlinebetrug – Abofallen und andere Hindernisse“: www.klicksafe.de/irights
- klicksafe: Schwerpunkt „Abzocke im Internet“: www.klicksafe.de/themen/einkaufen-im-netz/abzocke-im-internet/
- klicksafe-Flyer „Abzocke im Internet“ (in Deutsch, Türkisch, Russisch, Arabisch): www.klicksafe.de/materialien
- Übersicht aller deutschen Verbraucherzentralen: www.verbraucherzentrale.info

## 7 Jugendliche im Internet – die neue „Generation Sorglos“?

klicksafe/ Uwe Völkner

Schaut man sich die Inhalte und Informationen an, die Kinder und Jugendliche per Facebook, Messenger-App oder YouNow verbreiten, kann man sich als Erwachsener leicht wundern, wie offenherzig hier mit privaten Daten und den Daten von Freunden und Bekannten umgegangen wird. Woran aber liegt es, dass viele Kinder und Jugendliche (anscheinend) keine Probleme darin sehen, auch intimste Informationen im Internet zu veröffentlichen? Warum reagieren Kinder und Jugendliche auf die gut gemeinten Appelle von Eltern und Pädagogen zum Schutz persönlicher Daten vielfach mit Unverständnis?

Eine Antwort liegt bereits in der Struktur Sozialer Netzwerke. Wie oben bereits erwähnt, muss die Privatsphäre ein Stück weit aufgegeben werden, will man sich sinnvoll an Sozialen Netzwerken beteiligen. Eine Studie der Landesanstalt für Medien NRW (Heranwachsen mit dem Social Web, 2., unver. Aufl. 2011, S. 221) ergänzt in diesem Zusammenhang:

> „Für externe Beobachter erscheint oft bereits das Offenlegen bestimmter persönlicher Merkmale (wie Beziehungsstatus oder persönlicher Vorlieben) auf Netzwerkplattformen als Preisgeben der eigenen Privatsphäre; dieses Verhalten ist jedoch aus der kommunikativen Situation heraus nachvollziehbar: Nur durch das Ausfüllen eines eigenen Profils können Jugendliche an der Nutzergemeinschaft teilhaben, sich ihrer eigenen Identität und ihres Status innerhalb des Geflechts der online abgebildeten erweiterten Peer-Group bewusst werden und die Möglichkeit der Kommunikation mit den eigenen Freunden und Bekannten eröffnen.“

Darüber hinaus fällt es Jugendlichen – aber auch vielen Erwachsenen – schwer genau abzuschätzen, wer auf die eingestellten Bilder, Daten und Informationen tatsächlich zugreifen kann. Die oben genannte LfM-Studie (Kurzfassung unter www.lfm-nrw.de) ermittelte bei Jugendlichen und jungen Erwachsenen Fehleinschätzungen bezüglich der Reichweite, Nachhaltigkeit und Dynamik von Social Web-Angeboten. Umgeben von Freunden und Bekannten wähnen sich viele im sicheren Bereich einer geschlossenen Gruppe und sind entsprechend offenherzig. Dass auch der Anbieter oder staatliche Organisationen auf die eingestellten Daten zugreifen und dass Onlinefreunde und Bekannte die Informationen an andere Nutzer weitergeben könnten, wird hierbei häufig missachtet. Und bei einer durchschnittlichen Zahl von 256 befreundeten Community-Mitgliedern ist diese Wahrscheinlichkeit nicht gerade gering (JIM Studie 2014, S. 37ff.). Zudem wird in der jeweiligen Situation nicht immer bedacht, dass die als Momentaufnahme gedachten Informationen auch Jahre später immer wieder im Netz auftauchen können.

Als weitere Herausforderung kommen die durch mobiles Internet und Handykamera stark verkürzten Reflexionszeiten hinzu. So wurden die Zeiten, über mögliche negative oder ungewollte Folgen von verbreiteten Inhalten nachzudenken, noch einmal deutlich verkürzt. Nun können alle Inhalte gleich aus der Situation heraus mit einem Knopfdruck versendet werden (Stichwort „Impuls-Uploads"). Durch Apps wie Snapchat oder Slingshot, bei denen die versendeten Inhalte mit einer bestimmten Haltbarkeit versehen werden können, können Hemmschwellen zusätzlich sinken. (Hierbei ist wichtig zu betonen, dass die Inhalte über Screenshots oder spezielle Apps tatsächlich auch langfristig durch den Empfänger gesichert werden können.) Auch Angebote, mit denen Kinder und Jugendliche live in Echtzeit per Video mit anderen kommunizieren (zum Beispiel das auch als App erhältliche Angebot YouNow, siehe „Weitere Informationen"), schaffen im Sinne des Datenschutzes neue Herausforderungen.

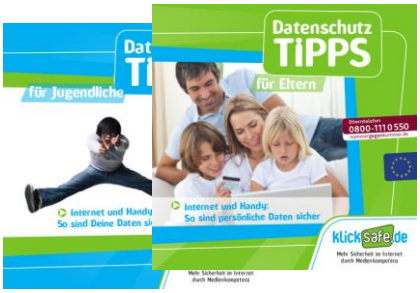
Unabhängig von diesen Aspekten wäre auch möglich, dass aktuell eine Generation heranwächst, die den Wert persönlicher Daten anders sieht bzw. die Grenzen zwischen Privat und Öffentlich weiter zieht, als z. B. das Gros der Generation ihrer Eltern (vgl. auch Kap. 10 „Fazit"). In diesem Fall müsste erst einmal ganz grundsätzlich versucht werden, eine Sensibilität für den Wert persönlicher Daten zu schaffen,

bevor konkrete Tipps zum Datenschutz vermittelt werden. Andernfalls würden diese auf wenig fruchtbaren Boden stoßen – und zwar unabhängig davon, ob mit oder ohne dem berüchtigten „erhobenen pädagogischen Zeigefinger" präsentiert.

**Weitere Informationen**

- klicksafe-Flyer „Sicherer in Sozialen Netzwerken: Tipps für Eltern" www.klicksafe.de/materialien
- Erklärvideo zu Snapchat unter: http://handysektor.de/navigation-paedagogen/paedagogenecke/videos.html
- Informationen zu YouNow gibt es unter: www.klicksafe.de/themen/kommunizieren/apps/younow/was-ist-younow/s/younow/ und www.lfm-nrw.de/index.php?id=3919

## 8 Tipps zum Schutz persönlicher Daten




Die folgenden Tipps zum Schutz von persönlichen Daten und zum Vorgehen bei Datenmissbrauch (Kapitel 9) sind dem klicksafe-Flyer „Datenschutz-Tipps für Eltern" (in Deutsch, Türkisch, Russisch und Arabisch veröffentlicht) entnommen bzw. an diesen angelehnt. Der Flyer „Datenschutz-Tipps für Jugendliche" kann in Gesprächen mit Kindern und Jugendlichen eine wichtige Hilfestellung liefern. Download und Bestellung über www.klicksafe.de/materialien.

- Überlegen Sie sich **vor dem Absenden** von Bildern und persönlichen Informationen, inwieweit eine Veröffentlichung oder Verbreitung problematisch sein könnte und wer auf die Informationen zugreifen kann.
- Prüfen Sie **AGB** und **Datenschutzrichtlinien** von Apps und anderen Diensten, bevor Sie sich zu einer Nutzung entscheiden. Machen Sie den App-Check unter www.klicksafe.de/apps.
- Überprüfen Sie regelmäßig Ihren "**Onlineruf**" in Sozialen Netzwerken und im Internet allgemein. Nutzen Sie neben "normalen" Suchmaschinen auch Personensuchmaschinen.
- Benutzen Sie **sichere Passwörter** (mindestens 8-stellig, Mischung aus Groß- und Kleinschreibung, Ziffern und Sonderzeichen), nicht immer das gleiche, und

ändern Sie es regelmäßig. Ein Passwort sollte nicht leicht zu erraten sein (also nicht der Name eines Haustieres, ein Spitzname oder ähnliches). Merksätze können dabei helfen, die Passwörter nicht zu vergessen.

- Geben Sie Passwörter nicht weiter. So wird bestmöglich verhindert, dass Fremde auf wichtige Daten zugreifen.
- Installieren Sie ein **Anti-Viren-** und ein **Anti-Spywareprogramm** auf Ihrem Computer und aktualisieren Sie diese regelmäßig.
- Schützen Sie Ihren Computer mit einer **Firewall** („Brandwand"). Eine Firewall schützt vor Angriffen und unberechtigten Zugriffen aus dem Internet und sollte nie ausgeschaltet werden.
- Sichern Sie Ihr **WLAN-Netzwerk** über eine verschlüsselte Verbindung (am besten WPA2). Wenn Sie unterwegs mit Handy, Tablet oder Laptop surfen, verschicken Sie möglichst keine wichtigen Daten und verzichten Sie auf Onlinebanking und ähnliche sensible Dienste.
- Schalten Sie **WLAN** und **Bluetooth** aus, wenn Sie es nicht benötigen.
- Führen Sie regelmäßig **Sicherheitsupdates Ihres Betriebssystems** durch. Auch Apps sollten immer auf dem aktuellen Stand sein. So werden Sicherheitslücken geschlossen.
- **Verschlüsseln** Sie Ihren E-Mail-Verkehr (siehe „Weitere Informationen").
- Öffnen Sie keine E-Mails mit **unbekanntem** Absender, vor allem keine **Dateianhänge**.
- Antworten Sie nicht auf **unerwünschte E-Mails** (Spam). Weitere nervige Mails wären die Folge! Am besten legen Sie sich zwei verschiedene E-Mail-Adressen zu. Eine geben Sie nur an gute Freunde und Bekannte weiter. Die andere verwenden Sie für Anmeldungen, Online-Shopping und so weiter.
- Bei jüngeren Kindern empfiehlt es sich, in einem **Mediennutzungsvertrag** festzuhalten, dass bestimmte persönliche Daten nur in Rücksprache mit den Eltern im Internet angegeben werden dürfen (siehe „Weitere Informationen"). Hierbei sollten konkrete Beispiele (z. B. Adresse, Nachname) festgehalten werden.
- Machen Sie Ihrem Kind das **lange Gedächtnis** des Internets klar und besprechen Sie, warum nicht alle Daten etwas im Internet verloren haben. In einigen Fällen kann die OMA-Regel bei der Auswahl helfen, nach dem Motto „Was würde meine Oma dazu sagen?"

- Sensibilisieren Sie Ihr Kind für den **fairen Umgang** mit Fotos und Daten von Mitschülern und Freunden. Jeder hat ein Recht auf Datenschutz!

**Weitere Informationen**


- Interaktiver Mediennutzungsvertrag von klicksafe und Internet-ABC: www.mediennutzungsvertrag.de
- Tipps zu sicheren Passwörtern: www.klicksafe.de/themen/datenschutz/privatsphaere/wie-sollte-ein-sicheres-passwort-aussehen/s/passwort/
- HEISE ONLINE: Tipps & Tools für anonymes Surfen: www.heise.de/download/special-tipps-tools-fuer-anonymes-surfen-151751.html
- Verbraucher sicher online: Themenbereich Verschlüsselung www.verbraucher-sicher-online.de/thema/verschluesselung

## 9 Was tun, wenn persönliche Daten missbraucht werden?

Die folgenden Tipps liefern in aller Kürze Hilfestellungen zum angemessenen Vorgehen beim Missbrauch von persönlichen Daten im (mobilen) Internet.

- Ist bekannt, wer die Inhalte veröffentlicht hat? Dann fordern Sie diese Person schriftlich dazu auf, die Inhalte bis zu einer von Ihnen festgelegten Frist zu entfernen.
- Wenn dies nichts bringt oder nicht möglich ist, wenden Sie sich an den Betreiber der Internetseite. Setzen Sie auch hier eine Frist. Sie finden die Kontaktdaten im Impressum oder über www.whois.net und www.denic.de. In Sozialen Netzwerken gibt es spezielle Melde-Buttons.
- Ist auch dies erfolglos, kann man sich bei Bedarf an einen Anwalt wenden. Auch die Datenschutzaufsichtsbehörde Ihres Bundeslandes kann je nach Situation helfen oder Ansprechpartner vermitteln.
- In schlimmen Fällen (schwere Beleidigungen, sehr problematische Bilder, die schnell entfernt werden sollen, …) sollten Sie auch die Polizei einschalten.
- Besprechen Sie mit Ihrem Kind, dass es auch Freunde und Bekannte informiert, wenn es im Internet komische oder peinliche Fotos und andere Infos von ihnen findet.

**Hinweis:**

- Wie betont, befinden sich per Handy und App versendete Inhalte nicht mehr „nur" auf dem Server des Anbieters – sie sind auf allen angeschriebenen Geräten gespeichert. Ein vollständiges Löschen ist so noch schwieriger als im Internet und meist sogar unmöglich. Betroffene müssen vielfach damit leben. Hier ist die soziale Unterstützung durch Familie, Freunde und Mitschüler umso wichtiger!

**Weitere Informationen**

- Experteninterview mit Philipp Otto und John Weitzmann von iRights.info (siehe Kapitel 11).
- Mehr zum Thema Datenschutz unter: www.klicksafe.de/themen/datenschutz
- klicksafe „Ratgeber Cyber-Mobbing – Informationen für Eltern, Pädagogen, Betroffene und andere Interessierte": www.klicksafe.de/materialien

## 10 Fazit

Schnelle Breitbandverbindungen, der Trend zum Mitmachnetz, der Überwachungsskandal rund um das Spähprogramm Prism und die zunehmende Nutzung des Internets über mobile Geräte haben dazu geführt, dass das Thema „Datenschutz" einen immer höheren Stellenwert hat. Zusätzlich werden Internetnutzer immer jünger und immer mehr Kinder und Jugendliche sind in Sozialen Netzwerken aktiv oder nutzen Messenger – zunehmend auch mobil. Auch aus diesem Grunde sollte möglichst früh mit Kindern über den Schutz persönlicher Daten gesprochen werden – eine Aufgabe die Schulen und Elternhaus gleichermaßen zuteilwird.

Aber selten hat der Nachwuchs hier das gleiche Problembewusstsein. Liegt dies aber wirklich nur daran, dass mögliche Folgen in diesem Alter noch nicht klar abgeschätzt werden können? Sind dies vielleicht auch erste Anzeichen dafür, dass sich die Grenzen zwischen dem, was als privat und was als öffentlich angesehen wird, zunehmend und möglicherweise dauerhaft verschieben? Eine Frage, die gleichzeitig spannend und in vielerlei Hinsicht entscheidend ist – v. a. in dem Sinne, inwieweit Kinder und Jugendliche über die vielfach gut gemeinten Appelle zum Schutz persönlicher Daten überhaupt noch erreicht werden können.

Unabhängig davon sollte das Thema „Datenschutz" aufgrund seiner enormen Bedeutung in der Erziehung frühestmöglich auf die Agenda gesetzt werden. Wie gezeigt wurde, werden Reichweite, Nachhaltigkeit und Dynamik eingestellter Informationen vielfach von Kindern und Jugendlichen unterschätzt und private Informationen entsprechend leichtfertig veröffentlicht. Dass neben Fairness im Umgang mit persönlichen Daten und Fotos anderer Nutzer auch Gesetze eine unautorisierte Veröffentlichung unterbinden, muss dem Nachwuchs ebenfalls mit auf den Weg gegeben werden.

Ein wichtiges Ziel wäre erreicht, wenn vor dem Klick auf „Jetzt Senden" noch einmal kurz geprüft werden würde, welche Folgen der Upload ggf. haben könnte und ob man mit den Infos auch Jahre später noch in Verbindung gebracht werden möchte.

## 11 Datenschutz im WWW – Ein Interview mit Philipp Otto und John Weitzmann von iRights.info

**F: Wo sehen Sie besondere Fallstricke, wenn es um das Thema „Datenschutz und Neue Medien" geht? Welche Auswirkungen haben die Neuen Medien auf den Bereich „Datenschutz"?**

Besondere Aufmerksamkeit muss beim Thema „Datenschutz und Neue Medien" auf Kauf- und Verkaufsvorgänge, die Nutzung von Suchmaschinen und die Nutzung von Sozialen Netzwerken gelegt werden. Bei kommerziellen Diensten gilt: Entweder wir bezahlen mit Geld, oder mit unseren Daten.

Beispielsweise beruht das Geschäftsmodell von Facebook darauf, dass möglichst viele Nutzer möglichst viele persönliche Daten preisgeben. Je mehr sie preisgeben, desto zielgerichteter können sie als Zielgruppe der Werbung angesprochen werden.

Datensparsamkeit ist eines der wichtigsten Prinzipien bei der Onlinenutzung. Daten können nur geschützt werden, wenn man sich darüber bewusst ist, was mit seinen Daten passiert, wenn man sie online eintippt. Nutzer tragen hier eine hohe Verantwortung.

Gleichzeitig müssen Unternehmen in Zukunft gezwungen werden, möglichst transparent über die Verwendung der Daten Auskunft zu geben und – dies ist alles andere als selbstverständlich – deutsche Datenschutzgesetze zu beachten. Hier gibt es noch viel Nachholbedarf.

**F: Gibt es gesetzliche Grenzen, wenn es um die Abfrage von persönlichen Daten geht – allgemein und speziell bei Kindern und Jugendlichen?**

Die Grundregel ist, dass nur in dem Umfang Daten erhoben werden dürfen, wie dies von einem Gesetz erlaubt wird oder soweit der Betroffene eingewilligt hat. Eine gesetzliche Erlaubnis gibt es z. B. immer dann, wenn ein Kunde eine Leistung haben will und dies nur mit Hilfe persönlicher Daten abgewickelt werden kann (Adress- und Zahlungsdaten).

Es gibt auf der anderen Seite keine „harte Grenze" dafür, wonach gefragt werden darf. Wird also nach sehr persönlichen Angaben gefragt, ist das für sich genommen noch nicht verboten. Wer diese Angaben dann bereitwillig macht, signalisiert damit zugleich, zumindest mit der Erhebung einverstanden zu sein – es sei denn, ihm wurde vorher unrichtigerweise suggeriert, zur Preisgabe seiner Daten verpflichtet zu sein.

Das alles betrifft aber erst einmal nur die Erhebung, also die Sammlung der Daten. Eine ähnliche Einwilligung braucht es zusätzlich für die Speicherung, Verarbeitung und Übermittlung der Daten an dritte Stellen. Hierin liegen oft erst die eigentlichen Gefahren. Besonders hierzu kommt es deshalb auf die „Datenschutzerklärung" des Datensammlers an und darauf, dass der Betroffene sie rechtzeitig zur Kenntnis nehmen kann und zugestimmt hat.

Für Kinder gilt insofern Besonderes, als dass sie erst dann rechtlich wirksam in irgendetwas einwilligen können, wenn sie die persönliche Reife erreicht haben, ihr Tun auch zu verstehen. Eine klare Altersgrenze gibt es nicht, aber Grundschulkinder verstehen normalerweise noch nicht, was eine Preisgabe von Daten bedeutet. Außerdem können sie ohne Zustimmung der Eltern auch noch keine Verträge schließen, deren Durchführung die oben genannte gesetzliche Erlaubnis zur Datensammlung mit sich bringen könnte. Werden Minderjährige mit der Zeit ver- und selbständiger, geht die Bedeutung der Zustimmung der Eltern entsprechend immer weiter zurück.

Ganz allgemein kommt Kindern wie Erwachsenen eine Sondervorschrift des Telemediengesetzes (TMG) zugute. Danach müssen Anbieter es immer dann ermöglichen, dass man ihre Dienste anonym oder unter Pseudonym nutzt, wenn das technisch möglich und zumutbar ist. Das trifft auf die meisten kostenlosen Dienste im Internet zu. Rechtlich nicht ganz klar ist, ob man deshalb bei solchen Diensten einfach Phantasie-Daten angeben darf, selbst wenn die AGB des Anbieters verlangen, dass man seine korrekten Daten angibt. Es dürfte einem solchen Anbieter jedoch sehr schwer fallen, die Nutzer rechtlich zu korrekten Angaben zu zwingen.

**F: Welche gesetzlichen Grenzen gibt es bei der Weiterverwertung der Daten?**

Erlaubnisse hinsichtlich Daten müssen immer getrennt von sonstigen AGBs eingeholt werden. Sofern die separate Datenschutzerklärung
a) alle relevanten Angaben enthält,
b) ausreichend eindeutig formuliert ist und
c) vom Betroffenen bewusst abgesegnet wurde
(oft fehlt es an einer dieser drei Voraussetzungen), gibt es ansonsten keine festgelegten Grenzen, was der Anbieter sich in der Datenschutzerklärung alles erlauben lassen darf. Schließlich umfasst die „informationelle Selbstbestimmung" auch das Recht, die eigenen Daten völlig freizugeben.

Allerdings ist die Einwilligung in die Datennutzung jederzeit ohne besonderen Grund widerrufbar, zumindest für die Zukunft. Ein Betroffener kann also jederzeit der weiteren Speicherung, Verarbeitung und Übermittlung seiner Daten widersprechen. Eine bereits geschehene Verarbeitung kann natürlich nicht mehr rückgängig gemacht werden, aber ihre Ergebnisse und die zugrundeliegenden Daten können gelöscht werden. Untersagt der Betroffene beim Widerruf der Einwilligung die weitere Speicherung, verlangt er damit im Zweifel zugleich die umfassende Löschung bereits erhobener Daten. Der Anbieter muss dieser Aufforderung nachkommen, wenn er nicht (z. B. zu Abrechnungszwecken bei einem Vertrag) ein besonderes Recht hat, die Daten aufzubewahren.

**F: Was müssen Schulen und Lehrerinnen und Lehrer in Sachen „Datenschutz und Neue Medien" beachten?**

Auch hier gilt der Grundsatz, dass nur solche Daten gesammelt werden dürfen, die durch das Schulgesetz für die Erfüllung der Aufgaben der Schule unerlässlich sind. Alles darüber hinaus bedarf der Einwilligung, bei kleineren Kindern durch die Eltern, bei größeren Kindern und Jugendlichen ist unter Umständen die eigene Einwilligung ausreichend. Darauf sollten sich Schulen aber möglichst nicht allein verlassen, sondern zusätzlich immer auch die Eltern fragen.

Bei Veröffentlichung von Daten im Internet ist die Schule dann in einem ganz anderen Bereich. Das ist sozusagen eine „Übermittlung an jedermann", die unbedingt

eine gesonderte Einwilligung braucht. Zudem können weitere sogenannte „besondere Persönlichkeitsrechte" tangiert sein, z. B. das Recht am eigenen Bild. Veröffentlichungen auf Schul-Homepages sollten also immer nur mit den nötigen Einwilligungen und so lange erfolgen, wie die betroffenen Schüler und ihre Eltern das wissen und einverstanden sind.

Schauen Lehrer umgekehrt übers Internet in die Profile, die ihre Schüler bei Social Networks wie Facebook anlegen, ist das datenschutzrechtlich unbedenklich. In einer rechtlich noch nicht ganz geklärten Zone bewegen sich Schulen bzw. Lehrer, wenn sie diese öffentlichen Informationen über ihre Schüler wiederum für sich sammeln, also irgendwo aufschreiben oder auf sonst eine Weise speichern. Da eine Schule nie wirklich sicher sein kann, dass sie dabei von der Einwilligung des Schülers gegenüber dem Social Network gedeckt ist, sollten solche indirekten Datensammlungen besser unterbleiben.

**F: Was kann ich tun, wenn ich feststelle, dass meine Daten oder die Daten meines Nachwuchses gegen meinen/seinen Willen oder sogar gesetzeswidrig verwendet oder weitergegeben worden sind?**
Dann sollte umgehend die sammelnde Stelle aufgefordert werden, die weitere Erhebung, Speicherung, Verarbeitung und Übermittlung der Daten zu unterlassen. Gibt es darauf keine Reaktion, kann mit einer sogenannten „Unterlassungsklage" gerichtlich vorgegangen werden. Schwierig wird das allerdings dann, wenn die sammelnde Stelle keinen Geschäftssitz in Deutschland hat und nicht einmal innerhalb der EU ansässig ist. Dann sollte man sich an den zuständigen Landesdatenschutzbeauftragten oder die Verbraucherverbände wenden, wo es speziell geschulte Juristen gibt, die solche Fälle genauer einschätzen können.

**F: Ab wann bzw. ab welchem Alter dürfen Kinder und Jugendliche selbst darüber entscheiden, welche Daten/Fotos sie im Internet veröffentlichen und weitergeben wollen?**
Wie oben bereits gesagt, hängt das von der sogenannten "Verstandesreife" ab. Über eigene Rechte können auch Minderjährige bereits in dem Maße selbst verfügen, wie sie die Implikationen ihres Handelns verstehen können. Für den Rest sind die Eltern zuständig.

Über die Jahre nimmt die Eigenverantwortlichkeit der Kinder immer mehr zu, die Zustimmungsrolle der Eltern immer mehr ab. Das sollte man allerdings nicht verwechseln mit der „beschränkten Geschäftsfähigkeit" Minderjähriger: Verträge, die irgendwelche Rechtspflichten erzeugen und die nicht mittels Taschengeld bereits erfüllt werden können, bleiben bei Minderjährigen so lange in einer Art Schwebezustand, bis die Eltern sie genehmigt haben. Soweit sich Datensammler also – ohne separate Erlaubnis – bei der Erhebung, Speicherung, Verarbeitung und Übermittlung der Daten einfach auf einen Nutzungsvertrag berufen wollen, können die Eltern diesen Vertrag jederzeit dadurch zu Fall bringen, dass sie die Genehmigung verweigern.

Private Datensammler können sich aber auch von Minderjährigen die Datennutzung durch eine vom sonstigen Vertrag separate Einwilligung erlauben lassen, soweit die Verstandesreife des Minderjährigen im Einzelfall reicht. Auch bei ausreichender Verstandesreife geht man heute für derlei Einwilligungen von einer Doppelzuständigkeit sowohl des Kindes wie der Eltern aus. Daher kann sowohl der Minderjährige ab dem achten Lebensjahr gegen eine Einwilligung der Eltern ein Veto einlegen als auch umgekehrt die Eltern gegen die Einwilligung ihres Sprösslings. Noch nicht endgültig geklärt ist in der Rechtsprechung, ob es neben der Einwilligung des Minderjährigen immer auch eine positive Einwilligung der Eltern braucht oder ob die Einwilligung des Minderjährigen ausreicht, solange kein aktives Veto der Eltern vorliegt.

**F: Was würden Sie Eltern von jüngeren Kindern zum Schutz persönlicher Daten im Internet mit auf den Weg geben?**

Eltern müssen zunächst sich selbst klarmachen, was es bedeutet, wenn bestimmte Daten verwendet werden. Hier gilt der Merksatz: Was man nicht mit Geld bezahlt, bezahlt man im Zweifel mit persönlichen Daten. Dieses Wissen sollten Sie ihren Kindern vermitteln. Dies kann im Sinne eines pädagogischen Warnhinweises geschehen, noch wirksamer ist aber, gemeinsam mit den Kindern die Relevanz und Bedeutung der Eingabe von Daten zu erarbeiten, zu diskutieren und Spielregeln festlegen.

Kinder sollen, sobald sie unsicher sind, sich mit ihren Fragen an ihre Eltern wenden können, ohne dass sie Angst haben müssen, etwas falsch gemacht zu haben oder gar bestraft zu werden. Das Wissen über die Bedeutung von Daten zu haben, ist kein Selbstläufer. Trotzdem sollte in der Erziehung und in der Einübung des Mediennutzungsverhaltens stark darauf geachtet werden. Selbst wenn die Rechtslage kompliziert und das Neu-Erlernen nicht ganz einfach ist.

**F: Habe ich ein Recht darauf, meine bei einem Anbieter gespeicherten Daten einzusehen und diese vollständig und dauerhaft löschen zu lassen?**
Ja, sowohl das Recht auf Auskunft über den Bestand an gespeicherten Daten als auch die Löschung ist im Bundesdatenschutzgesetz ausdrücklich gesetzlich verankert. Die Löschung kann ein Anbieter allenfalls dann verweigern, wenn er als Privater wegen eines Vertrages oder als staatliche Stelle wegen seines gesetzlichen Auftrags zur Speicherung bestimmter Daten berechtigt oder gar verpflichtet ist.

Bei Internetdiensten besteht das größere Problem meist darin, das Recht auf Auskunft und Löschung auch durchzusetzen. Wenn die jeweiligen Anbieter nicht in Deutschland oder der EU ansässig sind, ist an sie nur sehr schwer heranzukommen. Man sollte es dennoch versuchen und sich ggf. an den Landesdatenschutzbeauftragten oder die Verbraucherverbände wenden.

**F: Das Internet ist ein weltweites Netz. Welche Gesetze gelten bei im Ausland angesiedelten Anbietern und was ist hierbei zu beachten?**
Das Bundesdatenschutzgesetz gilt für alle Anbieter, die entweder in Deutschland oder außerhalb der EU bzw. des Europäischen Wirtschaftsraums (EWR) ansässig sind, aber hierzulande Daten erheben, verarbeiten oder nutzen. Bei den Anbietern dazwischen, die also in der EU oder dem EWR ansässig sind, gelten über internationale Abkommen die dortigen Datenschutzgesetze. Möchte man bei einem bestimmen Fall wissen, welche Regeln genau gelten, sollte man sich an Verbraucherverbände wenden.

Wie immer im Datenschutzrecht ist das größere Problem, die eigenen Rechte auch durchzusetzen. Man sollte darum

- die Datenschutzerklärungen von Onlinediensten genau lesen, bevor man Daten preisgibt,
- auch dann nur das Nötigste angeben,
- bei kostenlosen Diensten im Zweifel auch ausgedachte Daten angeben und
- die sehr freigiebigen Standardeinstellungen von Social Networks so anpassen, dass möglichst nur das weitergegeben wird, was man auch weitergeben möchte.

Wer auf Nummer sicher gehen will, sollte persönliche Daten nur an Onlinedienste solcher Anbieter geben, die in Deutschland oder der EU einen Sitz haben.

## Zu den Experten:

### Philipp Otto

Philipp Otto arbeitet als Berater, Wissenschaftler, Journalist und Verleger. Er ist Gründer und geschäftsführender Partner des Think Tank iRights.Lab und des Verlages iRights.Media. Er leitet die Redaktion des Onlinemagazins iRights.info und arbeitet in Kooperation mit vielen Partnern zu strategischen Fragen der Digitalisierung, der digitalen Agenda und ihrer Umsetzung. Seit knapp zehn Jahren beschäftigt er sich u.a. mit Netzpolitik. Er schreibt Strategiepapiere, Gutachten, Artikel sowie Aufsätze und ist u. a. Herausgeber des Jahresrückblick Netzpolitik. Zudem konzipiert und leitet er verschiedene weitere Projekte. Hin und wieder sitzt er auch in Hinterzimmern, auf einem Podium oder hält Reden.

### John Weitzmann

John Weitzmann ist in Berlin als Rechtsanwalt tätig und unterstützt die Redaktion irights.info. Er ist einer von zwei Europa-Koordinatoren für Creative Commons und engagiert sich zudem ehrenamtlich als Legal Project Lead für Creative Commons Deutschland. Regelmäßig veröffentlicht er Fachbeiträge zu Rechtsfragen in der digitalen Welt.

## 12 Linktipps

- **Internet-ABC: Themenbereich „Online-Communitys / Soziale Netzwerke"**
  In den einzelnen Artikeln zu Sozialen Netzwerken geht es immer wieder auch um den Datenschutz: www.internet-abc.de/eltern/online-communitys.php
- **klicksafe-Themenbereich „Datenschutz":**
  Der klicksafe-Themenbereich „Datenschutz" bietet Grundlagenwissen, ein Datenschutz-Dossier sowie Broschüren für Eltern und Jugendliche.
  www.klicksafe.de/themen/datenschutz
- **klicksafe-Unterrichtsmaterialien zum Thema „Datenschutz und Persönlichkeitsrechte im Web":** www.klicksafe.de/materialien
- **klicksafe-Quiz „Datenschutz für Jugendliche" – das Quiz zum Flyer „Datenschutz-Tipps für Jugendliche":** www.klicksafe.de/quiz
- **klicksafe-Informationen zu „Privatsphäre und Big Data":**
  www.klicksafe.de/themen/medienethik/privatsphaere-und-big-data/
- **klicksafe-Infos rund um Smartphone und Apps:**
  www.klicksafe.de/smartphones und www.klicksafe.de/apps
- **Broschüre „Smart mobil?!" von klicksafe und Handysektor:**
  www.klicksafe.de/materialien
- **Surfen ohne Risiko, Bereich „Daten schützen":**
  Informationen darüber, welche Daten gesammelt werden, wie man sorgsam mit Daten umgeht und welche Daten nicht ins Internet gehören usw.
  www.surfen-ohne-risiko.net/daten-schuetzen
- **KIM- und JIM-Studien, FIM-Studie des mpfs:**
  Die Studien des Medienpädagogischen Forschungsverbunds Südwest dokumentieren Daten und Informationen zur Nutzung, Funktion, Wirkung und den Inhalten von Medien. Download und Bestellung unter: www.mpfs.de.
- **Die schöne neue Welt der Überwachung:**
  Ein spielerischer und informativer Zugang zum Thema Datenschutz.
  www.panopti.com.onreact.com
- **Handysektor – Frische Infos zu Apps, Smartphones und Tablets:**
  www.handysektor.de
- **Handysektor – Das einfache Spiel der Datensammler:**
  www.handysektor.de/datenschutz-recht/datenschutz.html

- **Handysektor-Unterrichtseinheit zum Flyer „Das Netz vergisst nichts“:** www.handysektor.de/paedagogenecke
- **Videos "Think Before You Post":** www.smiley-ev.de/index.php?id=think_before_you_post
- **Infos und Tipps zum Thema „Datenschutz im Internet“:** www.datenparty.de
- **Virtuelles Datenschutzbüro**: www.datenschutz.de
- **WLAN und PC-Sicherung:**
  Informationen in Sachen WLAN und PC-Sicherung finden sich beispielsweise unter www.verbraucher-sicher-online.de und www.bsi-fuer-buerger.de.
- **Onlinespiel Data Dealer:**
  Ein jugendaffines Onlinespiel, welches sich kritisch und unterhaltsam mit dem Thema „Überwachung“ und „Schutz persönlicher Daten“ auseinandersetzt.
  www.datadealer.net