# DATENSCHUTZ IM NETZ AUF EINEN BLICK

**Im Netz sind mittlerweile fast alle und damit sind potentiell auch Informationen über viele Menschen im Netz, zum Beispiel Name, Porträtfoto oder Wohnort. Vieles wird freiwillig veröffentlicht, aber nicht wenige Daten gelangen unfreiwillig oder ohne Wissen der Nutzerinnen und Nutzer ins Internet und beginnen auf diese Weise ein „Eigenleben" in den Rechenzentren von Unternehmen oder sogar in der Netzöffentlichkeit.**

**„Datenschutz im Netz auf einen Blick" konzentriert sich auf Datenschutzfragen, die für das Internet relevant sind. Die Broschüre erläutert rechtliche Grundlagen des Datenschutzes in Deutschland, macht auf Probleme wie Profilbildung aufmerksam und gibt Tipps zum Umgang mit den eigenen Daten im Internet. Ideen zur Vermittlung von Datenschutzkompetenz sowie Literaturhinweise und Link-Tipps ergänzen das Informationsangebot.**

## WARUM DATENSCHUTZ?

Die Kreditkartennummer online eingeben, um einen Flug zu buchen, für Freundinnen und Freunde aus aller Welt über soziale Netzwerke erreichbar sein – das alles ist heute selbstverständlich und bietet Vorteile, die niemand mehr missen möchte. Aber egal ob Suchmaschine oder Community: Kein Webangebot ist wirklich kostenlos, denn die Nutzerinnen und Nutzer bezahlen für den Service mit ihren Daten. Dass sich daraus Nachteile oder Probleme ergeben können, zeigt sich in der Regel zunächst nicht.

Doch kaum eine Information ist uninteressant: Online-Zeiten lassen Rückschlüsse auf Arbeits- und Freizeitverhalten zu, Suchanfragen offenbaren Interessen, Standortdaten lassen sich zu Bewegungsprofilen verarbeiten, Online-Identitäten können missbraucht werden. Damit man im Internet nicht zum „gläsernen" Menschen wird, sich nicht auf Schritt und Tritt überwachbar macht, müssen insbesondere Behörden und Unternehmen in Deutschland Gesetze zum Datenschutz achten, Nutzerinnen und Nutzer verantwortungsvoll mit ihren Daten umgehen und besonders Internetunerfahrene über Datenschutzprinzipien und -probleme aufgeklärt werden.

### Grundsätze des Datenschutzrechts

Mit dem Durchbruch der elektronischen Datenverarbeitung drängten auch Fragen des Datenschutzes auf Be-

### *mekonet* Dokulinks

Mit seinem Dokulink-Service möchte *mekonet* Sie dabei unterstützen, komplexe Internetadressen leichter erreichen zu können, auf die wir in unseren Materialien hinweisen. Hinter dem Texthinweis „Dokulink" finden Sie jeweils eine zugehörige Nummer zum Angebot. Wenn Sie dieses Angebot aufrufen möchten, tippen Sie die Nummer in das Eingabefeld auf unserer Internetseite unter **www.mekonet.de/dokulink** ein. Sie werden dann automatisch zum entsprechenden Angebot weitergeleitet.

Alternativ können Sie den Dokulink auch direkt aufrufen, indem Sie nach **mekonet.de/d/** die jeweilige Nummer des Dokulinks in die Webadresse einfügen, also z. B. **mekonet.de/d/123456**.

### Material und Literatur (I)

Material

- Unter dem Motto „Ich bin öffentlich ganz privat" bietet klicksafe Informationen und Unterrichtsmaterialien zu Datenschutz und Persönlichkeitsrechten im Web für junge User. Außerdem erklärt klicksafe in seinen Leitfäden zur Kommunikation im Netz Schritt für Schritt, wie man sein Community-Profil sicher macht. **www.klicksafe.de**
- Zusammen mit dem Internet-ABC hat klicksafe einen Datenschutznewsletter für Eltern und Pädagogen zusammengestellt, der das Thema im Spiegel aktueller Entwicklungen wie Social Web, Online-Banking, mobile Dienste, Apps und Cloud-Computing diskutiert. **Dokulink 563394**
- A.G.F.A. – Apple, Google, Facebook und Amazon. Die Landesanstalt für Medien Nordrhein-Westfalen (LfM) erklärt in Ausgabe #5 von Digitalkompakt LfM die Strategien und Geschäftsmodelle der großen Vier im Internet (**Dokulink 165962**). Ausgabe #6 erklärt die große Wirkung kleiner Daten und bringt „Big Data" auf den Punkt (**Dokulink 128187**).

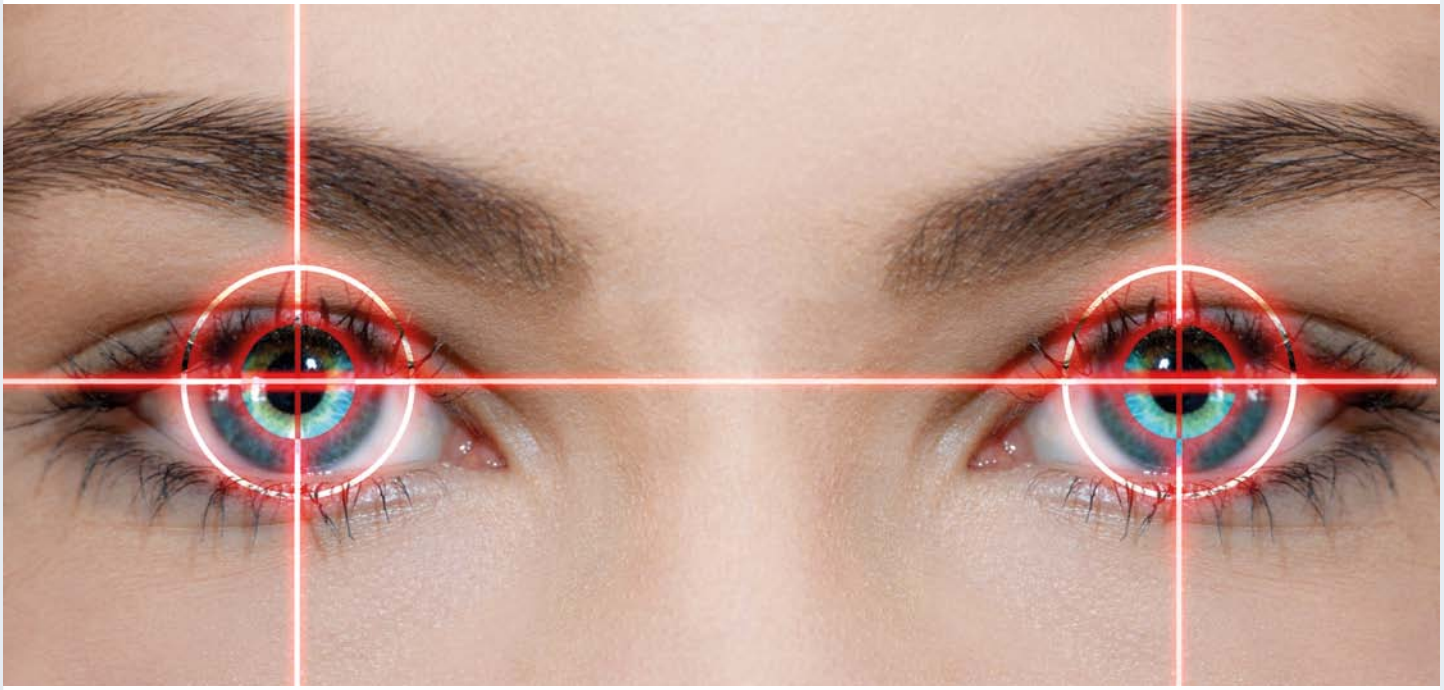
antwortung. Im **Volkszählungsurteil** legte das Bundesverfassungsgericht 1983 mit der Definition des Rechts auf informationelle Selbstbestimmung (BVerfGE 65, 1) die verfassungsrechtliche Grundlage für den Datenschutz in Deutschland.

Grundsätzlich sollen demnach jede Bürgerin und jeder Bürger über die Verwendung und Preisgabe der eigenen persönlichen Daten bestimmen können. Daraus und aus dem **Bundesdatenschutzgesetz**, das den Datenschutz insbesondere für Bundesbehörden und Unternehmen regelt, ergeben sich folgende Grundsätze:

- **Personenbezogene Daten** sind Informationen, die einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.
- Ohne **Einwilligung** oder Rechtsgrundlage dürfen keine personenbezogenen Daten erhoben, verarbeitet oder genutzt werden.
- **Für die Betroffenen muss transparent sein**, wer die Daten zu welchem Zweck verarbeitet.
- Nach dem Prinzip der **Datensparsamkeit und Datenvermeidung** sollen so wenige personenbezogene Daten wie möglich verarbeitet werden.
- Die Prinzipien der **Erforderlichkeit** und der **Zweckbindung** erlauben die Erhebung, Verarbeitung oder Nutzung von Daten nur so lange und in dem Umfang, wie die Daten notwendig sind, zum Beispiel zur Abwicklung eines Geschäftsvorgangs.
- **Auskunfts-**, **Widerrufs-**, **Berichtigungs-** und **Löschungsrechte** ermöglichen es den Betroffenen, sich jederzeit darüber zu informieren, welche Daten über sie verarbeitet wurden, die Einwilligung gegebenenfalls zurückzuziehen und personenbezogene Daten ändern oder löschen zu lassen.
- Über schwerwiegende **Datenschutzverletzungen**, zum Beispiel bei Datenpannen, sind die zuständigen Behörden sowie die Betroffenen und/oder die Öffentlichkeit zu informieren.

Soweit bei Telemedien (zum Beispiel bei Internetseiten) Bestands- oder Nutzungsdaten anfallen, finden datenschutzrechtliche Bestimmungen des **Telemediengesetzes** Anwendung. Nach dem **Telekommunikationsgesetz** sind Anbieter von Telekommunikationsdiensten (zum Beispiel Telefon, E-Mail, Internetzugang) darüber hinaus zur Wahrung des Fernmeldegeheimnisses verpflichtet. Dem **Fernmeldegeheimnis** unterliegen die Inhalte und die Umstände der Telekommunikation (zum Beispiel Informationen über beteiligte Personen, Ort und Zeit).

In einigen Fällen sind das Recht auf informationelle Selbstbestimmung und das Fernmeldegeheimnis mit den Interessen an einer effektiven Strafverfolgung und Verbrechensbekämpfung abzuwägen. Das Gesetz zur **Vorratsdatenspeicherung**, das die sechsmonatige anlasslose Aufzeichnung aller Verkehrsdaten (zum Beispiel IP-Adressen und Handyverbindungsdaten) anordnete, ist in Deutschland nach einem Urteil des Bundesverfassungsgerichts wieder außer Kraft. Dennoch können viele staatliche Stellen, Unternehmen und Privatpersonen die Herausgabe der zu betrieblichen Zwecken gespeicherten Verkehrsdaten von Telekommunikationsunternehmen erwirken. Bei Abmahnungen gegen Nutzerinnen und



Nutzer illegaler Musik- und Filmtauschbörsen ist dies gängige Praxis. Auch für Inhaltsdaten gibt es gesetzliche Regelungen, die unter engen Voraussetzungen eine Kontrolle ermöglichen, zum Beispiel durch Telekommunikationsüberwachung oder Online-Durchsuchung.

Nach **EU-Recht** ist die Übermittlung von Daten in Länder, die europäischen Datenschutzstandards nicht genügen, verboten. Hierunter fallen auch die USA. Ausländische Unternehmen, die – wie Facebook oder Google – die „**Safe-Harbor-Vereinbarung**" („Sicherer Hafen") unterzeichnet haben, können dennoch Daten aus der EU verarbeiten. Datenschützer kritisieren allerdings, dass die Kontrolle nicht gewährleistet ist und amerikanische Behörden im Zuge der Terrorbekämpfung sehr leicht auf Nutzerdaten zugreifen können.

## Datenschutzprobleme

Gesetzgebung und Rechtsprechung stehen angesichts der technischen Entwicklung des Internets vor Herausforderungen. Gesetzliche Bestimmungen in Deutschland werden gerade von internationalen Konzernen nicht immer eingehalten. Hier ist in vielen Fällen strittig, welches Recht überhaupt anzuwenden ist. Daraus ergibt sich eine Reihe von Problemen.

Gerade bei kostenlosen Angeboten gehen die erhobenen Daten oft über das Maß der Erforderlichkeit hinaus. Zum Beispiel greift eine App, die das Smartphone zur Taschenlampe macht, auf das Telefonbuch des Besitzers zu oder werten Web-Mail-Anbieter E-Mail-Inhalte aus. Hinter diesem Vorgehen steckt das Interesse der Anbieter, immer genauere Nutzerprofile zu erstellen, um sie für passgenaue Werbung zu nutzen oder sie weiter zu verkaufen. Zusammen werden die vielen kleinen Informationen über Surfgewohnheiten zu „Big Data" und erlauben zum Beispiel noch genauere Konsumvorhersagen. Während personalisierte Werbung oder Suchergebnisse noch im Interesse der Nutzerinnen und Nutzer sein können, kann die Profilanalyse durch Behörden, Krankenkassen, Banken oder Arbeitgeber erhebliche Nachteile bringen.

Nicht nur Datenpannen, Trojaner oder Datenabfang („Phishing") sorgen dafür, dass sensible Informationen wie Kreditkartennummern oder Passwörter in falsche Hände geraten, auch freiwillig veröffentlichte personenbezogene Daten lassen sich missbrauchen. Aus Namen, Geburtstag und Wohnort einer Person lässt sich eine gefälschte Online-Identität anlegen, die, „garniert" mit einem kopierten Bild aus einer Bildersuchmaschine, Kommentare postet, Beziehungen anbahnt oder dem Namen des Betroffenen in anderer Weise schadet. Hier reicht die Spanne von schlechtem Scherz bis zur Straftat.

Eine Reihe von Daten wird aber auch völlig ohne das Wissen der Betroffenen gesammelt. Kameras versehen Digitalfotos teilweise automatisch mit Informationen über den Aufnahmeort („Geo-Tagging"), die im Netz automatisch ausgelesen werden können. (Super-)Cookies oder so genannte Zählpixel sind kleine Dateien, die es ermöglichen, Computer, mit denen eine Website besucht wurde, wieder zu erkennen. Das gelingt auch über den „Fingerabdruck" des Browsers, der Informationen über das verwendete Betriebssystem, Sprache, Hard-

**Material und Literatur (II)**

- Auf **www.watchyourweb.de** finden Kinder Tipps zum sicheren Surfen und erfahren, wie sie sich vor Datenklau, Cybermobbing und Abzocke im Netz schützen können. Hier werden auch die Datenschutzeinstellungen und Erweiterungen für Browser erklärt.
- Auf **www.checked4you.de** informiert die Verbraucherzentrale Nordrhein-Westfalen junge Menschen über Verbraucherrechte und -fallen, die ihnen auch im Internet begegnen können.

Literatur


- Medienpädagogischer Forschungsverbund Südwest (2012): JIM-Studie 2012. Jugend, Information, (Multi-)Media. Basisuntersuchung zum Medienumgang 12- bis 19-Jähriger. Stuttgart 2012. **www.mpfs.de/?id=527**
- Pohlmann, Norbert und Markus Linnemann (2010): Sicher im Internet. Tipps und Tricks für das digitale Leben. Zürich. **Dokulink 633219**
- Schenk, Michael / Julia Niemann / Gabi Reinmann / Alexander Roßnagel (Hrsg.) (2012): Digitale Privatsphäre. Heranwachsende und Datenschutz auf sozialen Netzwerkplattformen. Berlin 2012. Schriftenreihe Medienforschung der Landesanstalt für Medien NRW (LfM), Band 71. Kompaktstudie. **Dokulink 392775**
- Die Broschüre „IM BLICKPUNKT: Informationelle Selbstbestimmung“ erklärt rechtliche Grundsätze zum Schutz personenbezogener Daten in Deutschland und zeigt Problembereiche auf. **Dokulink 128195**
- Die Broschüre „mekonet kompakt: Internetsicherheit auf einen Blick“ erläutert die wichtigsten Begriffe und Grundregeln, um das Surfen, Tauschen und den Handel im Internet sicherer zu machen. **Dokulink 388306**
- Broschüre von „Watch Your Web“ und iRights.info: Mein digitales Leben – Rechtliches kurz erklärt. **Dokulink 171438**


ware etc. an die besuchte Seite sendet. Diese Daten ermöglichen Profilbildung. Eindeutig einer Person zugeordnet werden können sie zum Beispiel dann, wenn man sich bei der besuchten Website mit seinem Klarnamen oder seiner E-Mail-Adresse anmeldet. Mobile Endgeräte merken sich, in welchen WLAN-Netzen sie unterwegs waren.

Viele Entwicklungen, die auf Datensammlung, -verknüpfung und intelligenter Auswertung beruhen, stehen erst am Anfang. Daten, die einmal gesammelt wurden, können auch noch in Jahren mit ganz neuen Technologien zu ganz anderen Zwecken eingesetzt werden.

## Datenschutzkompetenz als Medienkompetenz

Im Umgang mit privaten Daten im Netz stellt die Forschung ein so genanntes „Privacy Paradox“ (Niemann et al. 2012, 46) fest: Obwohl Nutzerinnen und Nutzer angeben, sich um ihre Privatsphäre im Netz zu sorgen, offenbaren sie viel Privates über sich. So schützen neun von zehn Jugendlichen ihre Online-Profile durch Privatsphäre-Einstellungen (JIM 2012, 43), während gleichzeitig die Gruppe der „Freunde“, mit denen Informationen geteilt werden, immer größer wird.

2012 umfasste die Kontaktliste von Jugendlichen über 270 Personen (JIM 2012, 45). Über die Hälfte der 12- bis 24-Jährigen sind online mit Personen vernetzt, die sie noch nie persönlich getroffen haben (Niemann et al. 2012, 224).

In der medienpädagogischen Arbeit gilt es daher, gerade Jugendlichen ein Gefühl für die Öffentlichkeit(en) zu vermitteln, in denen sie Informationen über sich preisgeben. Wer die Geschäftsmodelle hinter den Gratisdiensten versteht, kennt auch den Wert der eigenen Daten. Auch der respektvolle Umgang mit Informationen anderer, seien es Bilder, Kontaktdaten oder private Details, gehört zur Datenschutzkompetenz.

Einen Überblick über die Datenschutzkompetenzen, die in der medienpädagogischen Arbeit vermittelt werden sollten, bietet das Dossier „Mehr als Sicherheit: Datenschutz und Medienkompetenz – Wie hängt das zusammen?“ des Landesbeauftragten für Datenschutz und Informationsfreiheit NRW auf www.mekonet.de/dossiers. **Dokulink 156599**

## Wie die eigenen Daten schützen?

Wie hältst du’s mit dem Datenschutz? Das sollte man überhaupt jedes Online-Angebot fragen. Nachzulesen ist das in den Datenschutzerklärungen, in die man entweder beim ersten Anmelden einwilligen muss oder die sich auf der Website finden lassen. Die Verpflichtung, Nutzerinnen und Nutzer über die Datenschutzbestimmungen aufzuklären, ergibt sich für deutsche Anbieter aus dem Telemediengesetz. Achten sollte man darauf, ob

- personenbezogene Daten an Dritte weitergegeben werden und – wenn ja – an wen.
- die Möglichkeit besteht, die Weiterleitung von Daten abzulehnen,

- sich das Angebot Zugriff auf weitere auf dem Gerät gespeicherte Daten (zum Beispiel Adressbücher) verschafft,
- die Möglichkeit besteht, das Angebot auch ohne Anlegen eines Profils oder Eingabe von Daten zu nutzen,
- über die Form und Dauer der Datenspeicherung informiert wird,
- sensible Daten wie Kreditkarteninformationen verschlüsselt übermittelt werden (zum Beispiel durch Verwendung von SSL, zu erkennen am „https://" in der Adresszeile). Dies gilt auch für Daten, die man in Onlinespeicher (Cloud-Dienste) lädt,
- klar ist, wer für das Angebot verantwortlich ist und wie man mit der entsprechenden Stelle in Kontakt treten kann. Der Sitz des Anbieters kann auch darüber entscheiden, an welche Datenschutzgesetze er gebunden ist.

Entscheidet man sich dafür, zum Beispiel ein soziales Online-Netzwerk zu nutzen, sollte man sich zunächst überlegen, ob man mit seinem vollständigen Namen (Klarnamen) erscheinen möchte oder ob man per Nickname (Spitzname) anonym oder pseudonym unterwegs sein möchte, denn das Telemediengesetz erlaubt die anonyme oder pseudonyme Nutzung dieser Dienste. Im letzten Fall muss man sich dann natürlich auch mit einer E-Mail-Adresse anmelden, die keine Rückschlüsse auf die Person zulässt. Porträtfotos als Profilbild sind dann tabu.

Ein sicheres Passwort besteht nicht aus Wörtern oder Namen, die in Wörterbüchern stehen könnten, sondern aus Buchstaben, Zahlen und Sonderzeichen. Mit jedem weiteren Zeichen steigt die Sicherheit. Funktionen, wie die automatische Übermittlung von Positionsdaten sollten abgeschaltet werden, ebenso Funktionen wie „eingeloggt bleiben".

Viele Dienste laden Neuankömmlinge ein, möglichst viel über sich preiszugeben. Hier gilt es, lieber später nachzulegen als Eintragungen nachträglich zu entfernen. Sensible Informationen sollten nicht in Online-Netzwerken ausgetauscht werden, sondern eher über verschlüsselte E-Mails. Regelmäßiges Aufräumen in den gespeicherten Daten, das heißt Löschen von Nachrichten, Fotos oder Kontaktdaten gehört genauso zum Schutz personenbezogener Daten wie Passwörter zu wechseln und Privatsphäre-Einstellungen zu überprüfen. Mit der Einbindung von Suchfunktionen innerhalb sozialer Netzwerke wird dies noch wichtiger. Möchte man ein Angebot nicht mehr nutzen, löscht man alle hinterlegten Daten und das Benutzerkonto am besten vollständig.

### Tipps zum technischen Datenschutz im Netz

Um die personenbezogenen Daten vor unbefugtem Zugriff zu schützen, gibt es viele Möglichkeiten. In der Serie „Mein digitaler Schutzschild" testet ZEIT ONLINE Datenschutz- und Anonymisierungs-Tools, die Rückverfolgbarkeit auf eine Person erschweren oder ausschließen, und erklärt, wie man sie verwendet. **Dokulink 886658**

Datenschutz-Tuning für Browser: Unter „Einstellungen" kann man bei Firefox, Internet-Explorer, Chrome und Co. Hilfen wie die automatische Speicherung von Passwörtern oder Formulareingaben deaktivieren. Cookies und Verlauf (History/Chronik) sollte man automatisch regelmäßig löschen lassen. Wer allerdings gar keine Cookies akzeptiert, wird viele Websites nicht besuchen können. Die Firefox-Erweiterung (Add-On) „Better Privacy" schützt vor Langzeit-Cookies, die nicht automatisch gelöscht werden können. Tracking-Dienste wie Google-Analytics kann man über Browser-Erweiterungen wie „NoScript" oder „Ghostery" blockieren. **Dokulink 884763**

### Kontrolle und Unterstützung

Was ist zu tun, wenn beispielsweise ein Onlineshop, eine Bank oder eine Behörde gegen die datenschutzrechtlichen Bestimmungen verstößt? In Nordrhein-Westfalen wacht der Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) als Aufsichtsbehörde darüber, dass datenschutzrechtliche Vorschriften sowohl von Landes- und Kommunalbehörden als auch von der privaten Wirtschaft eingehalten werden. Bürgerinnen und Bürger können den Landesbeauftragten auf Datenschutzverstöße aufmerksam machen, auch wenn sie nicht persönlich betroffen sind.

**Landesbeauftragter für**
**Datenschutz und Informationsfreiheit**
**Nordrhein-Westfalen**
**Kavalleriestr. 2-4 • 40213 Düsseldorf**
**Postfach 20 04 44 • 40102 Düsseldorf**
**Tel.: 0211-38424-0**
**E-Mail: poststelle@ldi.nrw.de**
**Web: www.ldi.nrw.de**

Auf der Website des LDI NRW finden sich auch Hinweise, an welche Stellen man sich wenden kann, wenn das Datenschutzproblem nicht im Zuständigkeitsbereich des Landesbeauftragten liegt. **Dokulink 491163**

Die Aufsichtsbehörden gehen den Hinweisen nach und überprüfen den Vorwurf des Datenschutzverstoßes durch das jeweilige Unternehmen oder die Behörde. Sie können zum Beispiel gegenüber Unternehmen Maßnahmen zur Beseitigung festgestellter Verstöße anordnen. Bei schwerwiegenden Verstößen oder Mängeln können Bußgelder verhängt oder die Daten-Erhebung, -Verarbeitung oder -Nutzung oder der Einsatz einzelner Verfahren untersagt werden.

Hilfe bei „alltäglichen“ Fragen des Datenschutzes bekommen Privatpersonen bei den Verbraucherschützern. Der Bundesverband der Verbraucherzentralen (vzbv) mahnt Unternehmen zum Beispiel wegen unklarer Datenschutzregelungen ab und klagt gegen verbraucherfeindliche Praktiken. Mit dem Projekt „Surfer haben Rechte“ klärt der vzbv über Fragen des Datenschutzes auf und gibt Tipps zu Online-Shopping, -Communitys und anderen -Diensten (**www.surfer-haben-rechte.de**). Bei konkreten Fragen und Problemen zum Beispiel mit Online-Verträgen oder Abmahnungen beraten die Verbraucherzentralen in Nordrhein-Westfalen am Telefon, per E-Mail oder persönlich. **www.vz-nrw.de**

### Linktipps

- mekonet präsentiert unter **www.mekonet.de/quiz** ein Modul zum Thema Datenschutz, das vom Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen erarbeitet wurde.
- Mit dem nicht-kommerziellen Browserspiel Data-Dealer können User auf unterhaltsame Weise die Seiten wechseln und sich ihr eigenes Datenimperium aufbauen. **www.datadealer.net**
- Das Studentenprojekt panopti.com zeigt am Beispiel des Alltags von Paul, wo und wie wir täglich überwacht werden und wer Informationen über uns sammelt. **Dokulink 124128**
- Der Verein digitalcourage e.V. klärt über Datenschutzfragen auf und startet Aktionen gegen kritische Entwicklungen (**www.digitalcourage.de** und auf Twitter **@Digital_Courage**). Er verleiht alljährlich mit den Big Brother Awards den „Oscar für Datenkraken“. **www.bigbrotherawards.de**

### Noch Fragen?

Weiterführende Informationen und Links zum Thema Datenschutz im Internet finden Sie unter **www.mekonet.de** im Grundbaukasten Medienkompetenz unter dem Stichwort „Datenschutz & -sicherheit“ (**Dokulink 100827**). Oder fragen Sie das Projektbüro nach weiteren Literaturtipps.

## KONTAKT

*mekonet* – Medienkompetenz-Netzwerk NRW
Medienbildung für Multiplikatoren

Projektbüro *mekonet*
c/o Grimme-Institut
Gesellschaft für Medien, Bildung und Kultur mbH
Eduard-Weitsch-Weg 25
D-45768 Marl

Tel.: +49 (0) 2365 / 9189-61
Fax: +49 (0) 2365 / 9189-89

E-Mail: info@mekonet.de
Internet: www.mekonet.de

Facebook: facebook.com/mekonetnrw
Twitter: twitter.com/mekonet
Youtube: youtube.com/mekonetnrw

Ministerin für Bundesangelegenheiten, Europa und Medien des Landes Nordrhein-Westfalen

lfm: Landesanstalt für Medien Nordrhein-Westfalen (LfM)

Grimme Institut

LDI NRW Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen

Diese Handreichung wurde in redaktioneller Zusammenarbeit mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) und mit dessen finanzieller Unterstützung realisiert.

ClimatePartner° klimaneutral
Druck | ID: 10956-1304-1002



Stand: April 2013 – Fotos: Fotowerk (S. 1), Jürgen Fälchle (S. 3); alle Fotolia.com