Datenschutz TiPPS

für Eltern

Elterntelefon
0800-111 0 550
nummergegenkummer.de

internet und Handy:
So sind persönliche Daten sicher

klicksafe.de

Mehr Sicherheit im Internet
durch Medienkompetenz

Datenschutz TiPPS

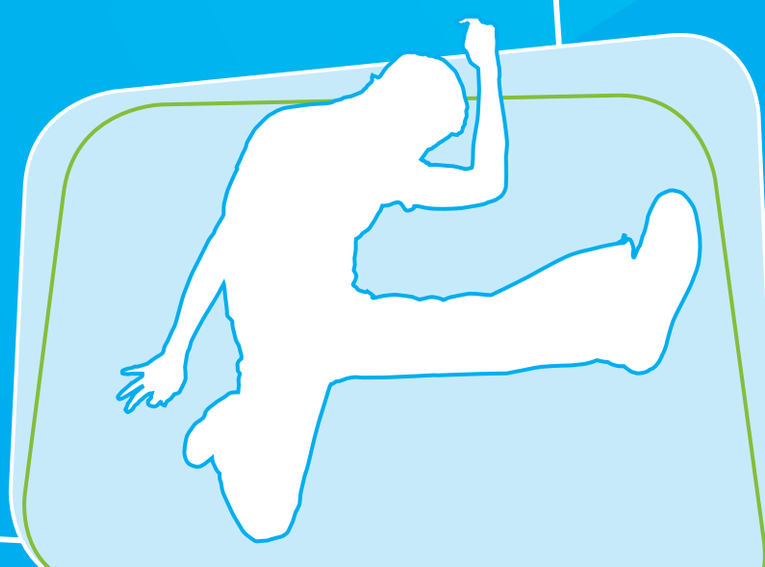
für Eltern

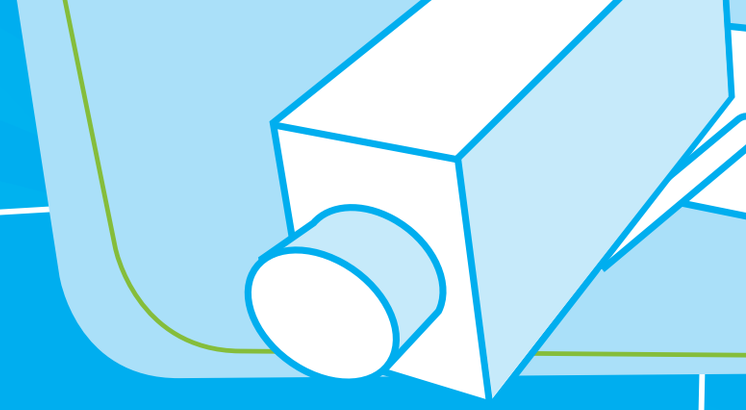
Liebe Eltern!
Viele Kinder und Jugendliche glauben, Datenschutz sei langweilig und gehe sie nichts an. Überzeugen Sie Ihr Kind vom Gegenteil!

Denn jeder Internet- und Handy-Nutzer hinterlässt Spuren. Manche Daten verraten die Nutzer freiwillig. Häufig merkt man aber auch gar nicht, dass persönliche Daten im Hintergrund gesammelt werden. Zum Beispiel greifen viele **Apps** (Spiele oder kleine Programme in Sozialen Netzwerken oder auf dem Handy) während der Nutzung auf persönliche Kontakte, das Telefonbuch oder andere Daten zu. Über mobile Geräte wird immer häufiger auch der aktuelle Aufenthaltsort abgefragt oder veröffentlicht. Zudem können bei Smartphones schneller problematische Inhalte (Fotos, Filme,...) aus der Situation heraus unüberlegt weitergeleitet oder veröffentlicht werden.

Der vorliegende Flyer will Ihnen dabei helfen, persönliche Daten im Internet und auf dem Handy bestmöglich zu schützen und das Thema „Datenschutz“ mit Ihren Kindern zu besprechen.

Ihr klicksafe-Team





1 Datenschutz macht Sinn

Persönliche Daten wie Adresse, Alter oder Telefonnummer nennt man auch „**personenbezogene Daten**“. Sie verraten viel über die eigene Person und bedeuten für Unternehmen bares Geld. Gerade sehr persönliche Informationen oder Fotos will wohl niemand offen im Netz oder auf beinahe allen Handys im Bekanntenkreis sehen. Datensparsamkeit macht also Sinn. Dies sollte auch jüngeren Internet- und Handy-Nutzern klar sein!

Besprechen Sie mit Ihrem Kind, dass per App versendete oder im Netz veröffentlichte Inhalte ab da nicht mehr privat sind. Nach dem Absenden hat man die Kontrolle über sie verloren. Die Inhalte können sich ungewollt auf andere Geräte verbreiten, in Suchmaschinen gelangen, kopiert werden und einen so immer wieder einholen. Dies rückgängig zu machen, ist nahezu unmöglich.

- Die schöne neue Welt der Überwachung: www.panopti.com.onreact.com
- Das Internet-Archiv „WayBack Machine“ speichert Webseiten als Zeitdokumente dauerhaft ab: www.archive.org.

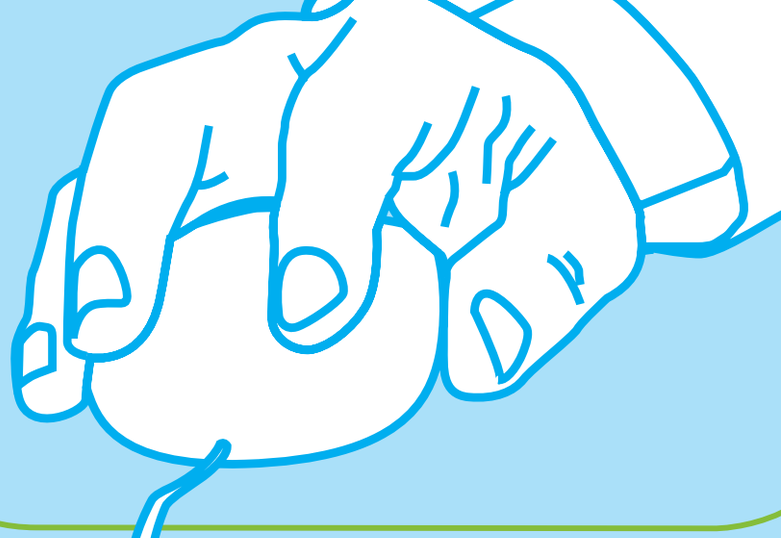
2 Datenschutz ist ihr gutes Recht

Durch das „**Recht auf informationelle Selbstbestimmung**“ sind persönliche Daten (Name, Adresse,...) in Deutschland sogar per Gesetz vor unerlaubter Verwendung geschützt. Das bedeutet: Niemand darf diese Daten ohne Einwilligung der betroffenen Person speichern, veröffentlichen oder weitergeben. Ausnahmen gibt es für einige staatliche Einrichtungen, wie zum Beispiel Meldeämter oder die Polizei.

Bei Fotos und Filmen gilt das „**Recht am eigenen Bild**“: Ausschließlich die abgebildete Person darf entscheiden, welche Bilder von ihr (z. B. in einem Sozialen Netzwerk) veröffentlicht oder verbreitet werden. Ausnahmen gelten für Bilder, auf denen man Teil einer Menschenmenge oder nur „Beiwerk“ ist. (Beispiel: Jemand fotografiert den Reichstag und Sie oder Ihr Kind stehen zufällig daneben.)

Übrigens: Ist Ihr Kind jünger als 12 Jahre alt, haben ausschließlich die Eltern/Erziehungsberechtigten bei Veröffentlichungen zu entscheiden. Zwischen 12 und 18 Jahren hängt es nach Meinung vieler Juristen vom Entwicklungsstand und der damit verbundenen Einsichtsfähigkeit des Kindes ab, ob es eigenverantwortlich über Bildveröffentlichungen entscheiden darf. **Tipp**: Tauschen Sie sich regelmäßig mit Ihren (jüngeren) Kindern über veröffentlichte und verschickte Fotos aus und bleiben Sie in Sachen „Datenschutz“ im Gespräch.

Checked4you - Deine Rechte im Web: www.checked4you.de (Passende Infos gibt es in den Themenbereichen „Computer + Internet“ und „Handy + Telefon“.)



3

Jeder hat ein Recht auf Datenschutz

Ihr Kind sollte nicht nur die eigenen, sondern auch die Persönlichkeitsrechte anderer beachten. Denn: Jeder hat ein Recht am eigenen Wort und am eigenen Bild. Machen Sie Ihrem Kind klar, dass es ohne deren Erlaubnis keine Bilder, Filme usw. von anderen per App weiterleitet oder im Netz veröffentlicht. Absolut verboten ist es, falsche Daten über jemanden zu verbreiten. Das wäre Rufschädigung und kann strafbar sein.

Tipp für ihr Kind: Denk nicht nur an Dich, beachte auch die Rechte anderer! Also keine Bilder, Filme oder private Infos von anderen Personen ins Netz stellen oder mit Apps weiterleiten – außer Du hast ihre Erlaubnis.

- Unter www.irights.info finden Sie weitere Infos zu Persönlichkeitsrechten und anderen Rechtsfragen in der digitalen Welt.
- www.handysektor.de: Im Bereich „Datenschutz + Recht “ gibt es passende Inhalte für Jugendliche.

4

So wird ihr Kind ein Datenprofi in Sozialen Netzwerken

Für den Schutz der eigenen Privatsphäre ist Ihr Kind auch selbst verantwortlich. Es sollte darauf achten, wie es sich in Sozialen Netzwerken zeigt! Geben Sie Ihrem Kind die folgenden **Tipps** mit auf den Weg:

- Ein Foto darf ruhig auch mal lustig sein. Allzu **peinliche** oder **beleidigende** Fotos oder Meinungen haben in Sozialen Netzwerken aber nichts zu suchen. Sie können auch Jahre später wieder im Netz auftauchen und Dich sogar den Ausbildungsplatz kosten.
- Überlege auch, was eine **Gruppenmitgliedschaft** über Dich aussagt. Die Gruppe „Saufen bis der Arzt kommt“ ist keine gute Werbung für Dich. Hassgruppen, in denen andere gezielt beleidigt werden, gehen gar nicht.
- Sei sorgsam mit Deinen **Profil-Daten**: Lass Anschrift, Handy-Nummer oder E-Mail-Adresse weg. Sie sind nicht nötig, wenn du Dich mit anderen austauschst.
- Überprüfe regelmäßig Deine **Privatsphäre-Einstellungen**. Hier helfen Dir die klicksafe-Leitfäden (siehe rechts). Aber auch strenge Einstellungen schützen nicht davor, dass berechtigte Kontakte Daten oder Fotos kopieren oder weiterleiten. Prüfe deshalb genau, wem du Zugang gibst. Du weißt nie, was andere mit den Inhalten machen!
- Nutzt Du Soziale Netzwerke unterwegs mit Deinem Handy? Dann achte besonders darauf, Bilder und Infos nicht vorschnell aus der Situation hochzuladen.

Wenn Ihr Kind ein Soziales Netzwerk nicht mehr nutzen will, dann sollte es seine Mitgliedschaft beenden und die dauerhafte Löschung des Kontos beantragen. So wird das Auffinden persönlicher Daten zumindest erschwert.

- Die „Leitfäden für die Kommunikation im Netz“ zeigen Schritt für Schritt, wie man Daten in Sozialen Netzwerken schützen kann. Hier gibt es auch einen Leitfaden zur Facebook-App: www.klicksafe.de/materialien.
- Infos zu Facebook gibt es unter: www.klicksafe.de/facebook.
- Zum persönlichen Schutz kann Ihr Kind auch das eigene Profilfoto witzig verändern: www.netzcheckers.de (unter „Workshops“).

5 Erst denken, dann klicken!

Internet und Handyspeicher haben ein langes Gedächtnis! Das heißt aber nicht, dass Ihr Kind ganz auf persönliche Informationen verzichten muss. Entscheidend ist die richtige Auswahl. Nachfolgend Tipps für Ihr Kind:

- Denk dran: Dinge, die Du heute über Internet und Handy austauschst, gefallen Dir in ein paar Jahren vielleicht überhaupt nicht mehr. Aber andere können sie immer wieder weiterleiten oder im Netz veröffentlichen.
- Überlege vor dem Absenden: Wie willst Du Dich anderen (im schlimmsten Fall) für immer zeigen? Was sollen andere von Dir wissen?
- Auch die „Oma-Regel“ kann Dir bei der Entscheidung helfen, nach dem Motto: Würde ich dies meiner Oma sagen oder zeigen?

- Videos „Think Before You Post“: www.smiley-ev.de/think_before_you_post.php

6 Elektronische Datenspuren hinterlässt man unbemerkt

- Technische Daten werden auch automatisch übertragen, ohne dass man es merkt. Gerade dies ist Kindern und Jugendlichen häufig nicht klar. Zwei Beispiele:
  - Viele Handy-Apps greifen im Hintergrund auf persönliche Daten wie das Telefonbuch oder den aktuellen Standort zu. Häufig ist dies nicht notwendig. Im Gegensatz zu Navigations-Apps muss zum Beispiel keine Taschenlampen-App wissen, wo man sich gerade aufhält. Da Nutzungsrechte bei App-Aktualisierungen erweitert werden können, sollte man diese regelmäßig prüfen (vgl. auch Punkt 12 links unten).
  - Das Kind besucht die Seite seiner Lieblingsband und sieht kurze Zeit später auf einer anderen Seite eine Werbung für ihre neue CD. Schuld daran können **Cookies** (wörtlich „Kekse“) sein. Cookies sind kleine Dateien, die auf dem Computer gespeichert werden. Sie „merken“ sich genau, welche Seiten besucht worden sind. So können Unternehmen den Internet-Surfer beobachten und herausfinden, welche Interessen er hat.

- Tipps zum Datenschutz bei Handys, Apps und in mobilen Netzen finden Sie unter www.handysektor.de, www.klicksafe.de und im Elternratgeber „Smart mobil?!“ von klicksafe und Handysektor.
- Mehr Informationen zum Thema „Cookies“ finden Sie auf www.klicksafe.de (Suchbegriffe: Cookies Spyware).

7 Nicknames nutzen – unerkannt surfen

Ein guter **Nickname** („Deckname“) kann dabei helfen, im Internet unerkannt zu surfen. Hierbei ist Erfindungsgeist gefragt. Ein Deckname der dem richtigen Namen zu ähnlich ist oder das Alter enthält, hilft wenig. Ihr Kind kann ihn zum Beispiel in Blogs, Chats und Foren benutzen. Machen Sie Ihrem Kind auch klar, dass es sich nicht hinter einem Nick verstecken oder sich als jemand anderer ausgeben soll, um andere gezielt zu beleidigen. Das ist unfair und kann sogar bestraft werden!

! Je häufiger Ihr Kind im Internet unterwegs ist, umso sicherer ist es, wenn es verschiedene Nicks verwendet. So haben Beleidigungen, Betrug und anderer Datenmissbrauch eine geringere Chance.

8 So behält ihr Kind die Kontrolle über seine Daten

Je mehr persönliche Daten Ihr Kind im Internet veröffentlicht oder per Handy verschickt, umso weniger können diese kontrolliert werden. **Datensparsamkeit** lohnt sich und schützt vor bösen Überraschungen. Gemeinsam mit Ihrem (jüngeren) Kind können Sie entscheiden, welche persönlichen Daten es ohne Probleme veröffentlichen oder weiterleiten darf. Fragen Sie Ihr Kind, ob es seine Daten (noch) im Griff hat!

Häufig verbreiten aber auch andere Personen private Dateien, Informationen oder Fotos von Ihrem Kind. Aus diesem Grunde sollte der eigene „**Online-Ruf**“ regelmäßig in verschiedenen Suchmaschinen geprüft werden. In Sozialen Netzwerken sollte man Profile und Fotoalben von Freunden nach Inhalten, die die eigene Person betreffen, prüfen und ggf. um Entfernung bitten. Wenn unerwünschte Inhalte des eigenen Kindes auf Handys in der Schule die Runde machen, sollte man sich rechtzeitig und in Rücksprache mit dem eigenen Kind an die Schule wenden. Gemeinsam kann dann ein Vorgehen abgestimmt werden (siehe Punkt 11 rechts unten).

Personensuchmaschinen: www.yasni.de, www.123people.de

9 Die AGB – Was der Anbieter mit den Nutzerdaten machen darf

Gerade Kindern und Jugendlichen fällt es häufig schwer, die **AGB**, die Allgemeinen Geschäftsbedingungen eines Angebots, zu lesen und zu verstehen. Vor allem die hier enthaltene **Datenschutzerklärung** ist überaus wichtig und sollte genau studiert werden. Dort erfährt man, was mit den Nutzerdaten passiert, was gespeichert, weitergegeben oder für Werbung genutzt wird. Und mit einer Anmeldung stimmt man den AGB automatisch zu! **Tipp**: Verabreden Sie mit Ihrem (jüngeren) Kind, dass Sie neue Internet-Angebote oder Apps vorab gemeinsam anschauen und prüfen. Sagen Sie Ihrem Kind, dass es sich bei Fragen jederzeit an Sie wenden kann. Im Zweifel sollte Ihr Kind lieber auf eine Nutzung verzichten – auch wenn es häufig schwerfällt.

Zwei Beispiele von vielen:

- Viele kostenlose Apps finanzieren sich über Werbeeinblendungen. Hier sollte man genau prüfen, auf welche Inhalte die App zugreift (siehe auch Punkt 6) und für welche Angebote Werbung geschaltet wird.
- Viele kostenlose **E-Mail-Anbieter** „lesen“ die Inhalte von E-Mails automatisch nach Schlüsselwörtern aus, um dem Nutzer dazu passende Werbung zu senden.

Auf www.handysektor.de finden sich unter „Datenschutz + Recht“ altersgerechte Informationen für Jugendliche.

10 Umsonst ist nicht kostenlos

- Viele Apps oder Angebote wie Suchmaschinen und Soziale Netzwerke sind auf den ersten Blick kostenlos. Tatsächlich funktioniert das Geschäftsmodell aber so, dass die gespeicherten oder versendeten Daten ausgewertet und für Werbung genutzt werden. Je nach Interessen, Alter oder Geschlecht werden dann möglichst passende Werbeinhalte in der App oder auf der Webseite eingeblendet. So wird wahrscheinlicher, dass die Werbung angeklickt wird oder Wirkung zeigt.
  Tipp: Sprechen Sie mit Ihrem Kind über Online-Werbung. Erklären Sie, warum Unternehmen möglichst viel über ihre Zielgruppe erfahren wollen. Prüfen Sie gemeinsam, woran man Werbung im Internet oder in Apps erkennt. Besprechen Sie auch, dass ein Klick auf Werbung zu problematischen Inhalten oder zu Abzockseiten führen kann.

- Weitere Informationen gibt es im Eltern-Leitfaden „Internetkompetenz für Eltern“ und im Flyer „Abzocke im Internet“: www.klicksafe.de/materialien.
- Mehr Infos zum Thema „Werbung“ gibt es auf www.klicksafe.de. (Klicken Sie auf „Themen“, dann unten links auf „Werbung“.)

11 Tipps: Richtig reagieren bei Datenmissbrauch

- Verbreiten sich unerwünschte persönliche Daten, Infos oder Bilder, dann gehen Sie dagegen vor. Beziehen Sie das betroffene Familienmitglied mit ein, um Missverständnisse zu vermeiden. Sagen Sie Ihrem Kind auch, dass es sich bei solchen Problemen immer an Sie wenden kann.

- 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.

! Inhalte, die über Handy und Apps versendet werden, befinden sich nicht mehr „nur“ auf dem Server des Anbieters – sie befinden sich auf allen angeschriebenen Geräten. 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!

12

Sicherheitstipps – So sind die Daten ihrer Familie gesichert

- Benutzen Sie **sichere Passwörter** (mindestens achtstellig, Mischung aus Groß- und Kleinschreibung, Ziffern und Sonderzeichen) und nicht immer das gleiche. Ein Passwort sollte nicht leicht zu erraten sein (also nicht der Name eines Haustieres, ein Spitzname usw.). Merksätze können dabei helfen, die Passwörter nicht zu vergessen. Passwörter sollten zudem regelmäßig geändert werden.
- Erklären Sie Ihrem Kind, warum es Passwörter nicht weitergeben sollte. So wird verhindert, dass Fremde auf wichtige Daten zugreifen können.
- Installieren Sie ein **Anti-Virenprogramm** auf Computer und Smartphone und aktualisieren Sie es 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 (möglichst WPA2). Von unterwegs sollte man beim kabellosen Surfen mit Smartphone oder Tablet keine wichtigen Daten verschicken.
- Schalten Sie **WLAN** und **Bluetooth** aus, wenn sie nicht benötigt werden.
- Führen Sie regelmäßig **Sicherheits-Updates** (Update=Aktualisierung) von Betriebssystem, Programmen und Apps durch. So werden Sicherheitslücken geschlossen. Prüfen Sie beim Handy vor dem Update von Apps, ob Zugriffsrechte unnötig erweitert werden. Apps sollten deshalb nicht automatisch aktualisiert werden.

- Sagen Sie Ihrem Kind, dass es keine E-Mails mit **unbekanntem** Absender öffnen sollte, vor allem keine mitgeschickten Dateien.
- Auf unerwünschte Nachrichten sollte man nicht antworten. Weitere nervige Anfragen wären die Folge! Ob bei E-Mails oder Sofortnachrichten – besser ist es, den Absender zu blockieren.

Legen Sie jedem Familienmitglied **zwei E-Mail-Adressen** an. Eine nutzt man für Freunde und Bekannte. Die andere verwendet man für Anmeldungen, Online-Shopping und so weiter.

- www.handysektor.de: Infos zum Thema „Sicherheit in mobilen Netzen“
- www.klicksafe.de: Unter „Themen – Datenschutz“ finden Sie weitere Infos und ein spannendes Quiz zu diesem Flyer, welches Sie gemeinsam mit Ihren Kindern spielen können (siehe unten). Das Quiz kann auch ein guter Aufhänger sein, um über das Thema „Datenschutz“ ins Gespräch zu kommen.
- Das Quiz „Smart mobil“ (www.klicksafe.de/quiz) eignet sich als Einstieg im Bereich „mobiles Internet“.

Bist Du ein Datenprofi?

Mach das Quiz unter
www.klicksafe.de/quiz.

klicksafe ist Partner im deutschen Safer Internet Centre der Europäischen Union.

klicksafe sind:

LMK Landeszentrale für Medien und Kommunikation Rheinland-Pfalz

Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz – www.lmk-online.de

lfm: Landesanstalt für Medien Nordrhein-Westfalen (LfM)

Landesanstalt für Medien Nordrhein-Westfalen (LfM) – www.lfm-nrw.de

Coverfoto: © WavebreakMediaMicro - www.fotolia.com

Herausgeber:

klicksafe
c/o Landesanstalt für Medien
Nordrhein-Westfalen (LfM)
Zollhof 2
D-40221 Düsseldorf

T: +49 (0)211-77 00 7-0
F: +49 (0)211-72 71 70
E: klicksafe@lfm-nrw.de
W: www.klicksafe.de

klicksafe wird kofinanziert von der Europäischen Union

- 4. vollständig aktualisierte Auflage 2014 -