Datenschutz TIPPS

für Jugendliche

Kinder- und Jugendtelefon
0800-111 0 333
nummergegenkummer.de

internet und Handy:
So sind Deine Daten sicher

klicksafe.de

Mehr Sicherheit im Internet
durch Medienkompetenz

Datenschutz-TiPPS

für Jugendliche

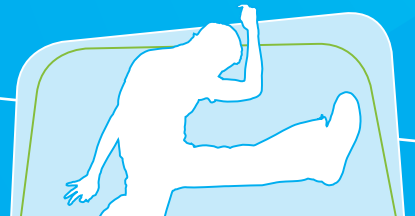
Du glaubst, Datenschutz ist langweilig und geht Dich nichts an? Lass Dich vom Gegenteil überzeugen!

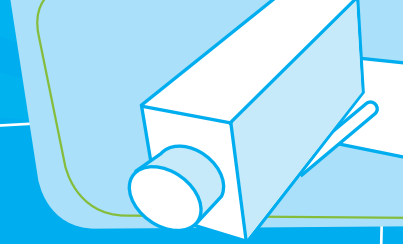
Wenn Du im Internet surfst oder Dein Handy nutzt, hinterlässt Du Datenspuren. Manches verrätst Du freiwillig. Häufig merkst Du aber auch gar nicht, dass persönliche Daten von Dir gesammelt werden. Zum Beispiel greifen viele Apps während der Nutzung auf Deine Kontakte, Deine Fotos, Deinen Standort oder andere Daten zu.

Aber nicht alle Informationen über Dich und Dein Leben gehen jeden etwas an, oder?

Wir sagen Dir, was Du für den Schutz Deiner Daten tun kannst.

Dein klicksafe-Team





1 Datenschutz macht Sinn

Persönliche Daten, zum Beispiel Deine Adresse, Dein Alter oder Deine Interessen, nennt man auch **personenbezogene Daten**. Sie verraten viel über Dich, sind kostbar und können von anderen missbraucht werden.

Du könntest jetzt denken: Was soll's, ich habe doch nichts zu verbergen! Aber bestimmt fallen auch Dir Bilder oder Informationen ein, die nicht offen im Internet oder auf fremden Handys zu finden sein sollen (zum Beispiel die Geheimzahl Deines Kontos oder Dein Babyfoto mit rotem Kopf in der Badewanne;-)).

Denk daran: Einmal versendet, beginnen Deine Daten ein **Eigenleben**. Sie werden kopiert, verbreitet und tauchen so immer wieder auf. Deshalb haben Internet und Handyspeicher oft ein sehr langes **Gedächtnis**. Und Dinge, die Du heute gut findest, gefallen Dir in ein paar Jahren vielleicht überhaupt nicht mehr. Aber im Internet und auf fremden Handys gibt es sie dann immer noch. Datenschutz macht also Sinn!

- Die schöne neue Welt der Überwachung www.panopti.com.onreact.com
- Infos zum Thema „Datenschutz, Apps und Smartphones" gibt es auf www.handysektor.de.

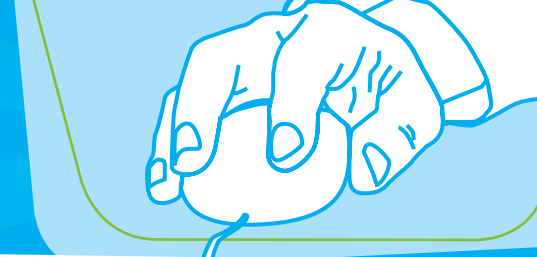
2 Datenschutz ist Dein gutes Recht

Durch das **Recht auf informationelle Selbstbestimmung** sind Deine persönlichen Daten (Name, Adresse, usw.) sogar per Gesetz geschützt. Das bedeutet: Niemand darf diese **ohne** Deine Einwilligung speichern, veröffentlichen oder weitergeben. Ausnahmen gelten zum Beispiel für Meldeämter oder die Polizei.

Was gilt für Fotos und Filme? Hier gibt es das **Recht am eigenen Bild**: Du entscheidest, welche Bilder von Dir **veröffentlicht** oder **verbreitet** werden dürfen. Ein Bekannter darf also nicht einfach so ein Bild von Dir in einem Sozialen Netzwerk hochladen.

Übrigens: Bist Du jünger als 12 Jahre, musst Du Deine Eltern (oder Erziehungsberechtigten) vor dem Hochladen eines Fotos fragen. Aber auch danach solltest Du Dir **vorher** überlegen, was das Bild über Dich aussagt und ob es Dir in ein paar Jahren vielleicht peinlich sein könnte.

www.checked4you.de – Deine Rechte im Web (Klick im Bereich „Themen“ unter dem Punkt „Computer + Internet“ auf „Internet“.)



3 Sei fair mit den Daten anderer

Denk nicht nur an Dich. Beachte auch das Recht auf Datenschutz und Privatsphäre von anderen!

Also keine Bilder, Filme oder private Daten von anderen per App weiterleiten oder im Internet veröffentlichen – außer Du hast ihre Erlaubnis. Zu privaten Daten gehört auch der aktuelle Aufenthaltsort einer Person.

Absolut verboten ist es, bewusst falsche Daten über jemanden zu veröffentlichen. Das kann sogar strafbar sein.

Unter www.irights.info findest Du weitere Infos zum Thema „Urheber- und Persönlichkeitsrechte in der digitalen Welt“.
Auf www.medien-knigge.de werden Umgangsformen in der neuen Medienwelt vorgestellt.

4

Sei ein Datenprofi in Sozialen Netzwerken

Achte darauf, wie Du Dich in Sozialen Netzwerken zeigst! Hierbei helfen folgende Tipps:

- Ein Foto darf ruhig auch mal lustig sein. Allzu **peinliche** oder **beleidigende** Fotos oder Meinungen haben in Sozialen Netzwerken aber nichts zu suchen.
- Überlege auch, was eine **Gruppenmitgliedschaft** über Dich sagt. 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 **Profildaten**: Lass private Infos wie Anschrift, Handynummer oder E-Mail-Adresse lieber weg. Sie sind nicht nötig, wenn Du Dich mit anderen austauschst.
- Überprüfe regelmäßig Deine **Privatsphäre-Einstellungen**. Hier helfen Dir die klicksafe-Leitfäden (siehe unten).
- Prüfe genau, wem Du freien Zugang zu Deinen **privaten** Fotos und Daten gibst. Du weißt nie, was sie mit den Informationen machen!

- Die klicksafe-Leitfäden für mehr Sicherheit auf Facebook findest Du unter www.klicksafe.de/facebook.
- Ein Workshop auf www.netzcheckers.de zeigt Dir, wie man zum persönlichen Schutz Profilbilder witzig verändern kann.

5

Erst denken, dann senden

Häufig gilt, dass Internet und Handyspeicher nicht vergessen. Das heißt aber nicht, dass Du ganz auf persönliche Infos verzichten musst. Entscheidend ist die richtige Auswahl. Hier helfen Dir folgende Tipps:

- 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?
- Nutzt Du Soziale Netzwerke oder Apps wie WhatsApp, Threema oder Instagramm mit Deinem Handy? Dann achte darauf, Bilder und Infos nicht vorschnell aus der Situation heraus zu versenden. Besonders unterwegs gilt: **Erst denken, dann senden!**

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

6 Elektronische Datenspuren hinterlässt Du unbemerkt

- Technische Daten werden auch automatisch im Hintergrund übertragen, ohne dass Du es merkst. Zwei Beispiele:
  - Viele Handy-Apps greifen auf persönliche Daten wie Deine Kontakte oder Deinen aktuellen Standort zu. Häufig ist dies nicht notwendig. So muss keine Taschenlampen-App wissen, wo Du Dich gerade aufhältst. Da Apps **Zugriffsrechte** bei Aktualisierungen ändern können, sollte man diese regelmäßig prüfen und Updates nicht automatisch durchführen lassen.
  - Du besuchst die Internetseite einer Band. Später poppt Werbung für ihr neues Album auf. Schuld daran können Cookies (wörtlich „Kekse“) sein. Das sind kleine Dateien, die auf Computer oder Handy gespeichert werden. Sie merken sich, was Du Dir im Internet angeschaut hast. So können Unternehmen herausfinden, welche Interessen Du hast.

- Tipps zum Datenschutz bei Handys und Apps findest Du unter www.handysektor.de und unter www.klicksafe.de/apps.

7 Nutze Nicknames und surfe unerkannt

- Ein guter **Nickname** („Deckname“) kann Dir dabei helfen, im Internet unerkannt zu surfen. So bietest Du weniger Angriffsfläche für Beleidigungen, Abzocke und anderen Datenmissbrauch. Sei hierbei **erfinderisch**! Der Nickname sollte Deinem richtigen Namen nicht zu ähnlich sein oder Dein Alter enthalten. Verwende ihn zum Beispiel in Chats oder Foren.

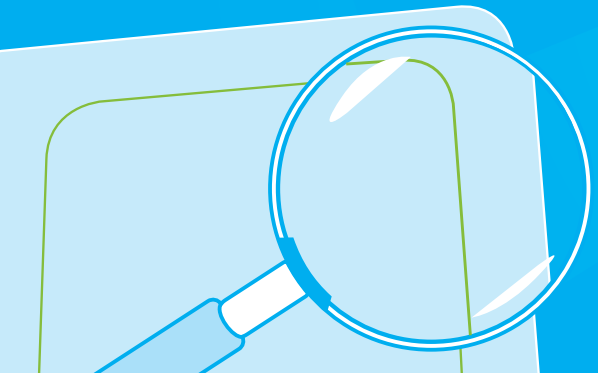
- Verstecke Dich aber nicht hinter Deinem Nickname oder gib Dich als jemand anders aus, um andere gezielt zu beleidigen. Behandele andere auch in der digitalen Welt so, wie Du selbst behandelt werden willst: mit **Respekt**!

8 Behalte die Kontrolle über Deine Daten

Je mehr Daten Du von Dir verrätst, umso weniger **Kontrolle** hast Du darüber. Manchmal haben aber auch andere etwas über Dich veröffentlicht – und nicht immer merkt man es.

- Wie steht's um Deinen **digitalen Ruf**? Gib Deinen Namen in verschiedene Suchmaschinen ein.
- Prüfe die Profile und Fotoalben Deiner Freunde, wie Du dort erscheinst. Bitte bei Bedarf darum, Dich störende Bilder von Dir zu entfernen.
- Wenn unerwünschte Inhalte von Dir auf Handys die Runde machen, bitte eine erwachsene Vertrauensperson um Unterstützung.

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



9 Die AGB – Was der Anbieter mit Deinen Daten machen darf

Oft schwer zu lesen, aber trotzdem wichtig: die **AGB**, die Allgemeinen Geschäftsbedingungen von Internetangeboten oder Apps. Sie enthalten auch eine **Datenschutzerklärung**. Hier erfährst Du, was mit Deinen Daten passiert, also was gespeichert, weitergegeben oder für Werbung genutzt wird.

Mit Deiner Anmeldung stimmst Du den AGB automatisch zu! Schau sie Dir deshalb vorher genau an. Wenn Du sie nicht verstehst, frage Eltern oder ältere Geschwister um Hilfe. Im Zweifel lieber auf eine Anmeldung verzichten – auch wenn es häufig schwerfällt.

Hier **zwei Beispiele** von vielen:

- Viele kostenlose **Apps** finanzieren sich über Werbung. Deshalb sollte man vor der Installation genau prüfen, wie die App bewertet ist und auf welche Daten die App zugreift (siehe auch Punkt 6). Bei der Einschätzung einer App hilft Dir der **App-Check** unter www.klicksafe.de/apps.
- Viele kostenlose **E-Mail-Anbieter** lesen die Inhalte Deiner E-Mails nach Schlüsselwörtern aus, um Dir dazu passende Werbung zu senden.

Auf www.handysektor.de findest Du unter „Apps + Upps" auch den **App-Alarm**. Hier kannst Du Apps vorschlagen, die vom Handysektor getestet werden.

10 Umsonst ist nicht kostenlos

Viele Apps, Suchmaschinen oder Soziale Netzwerke sind auf den ersten Blick kostenlos. Tatsächlich zahlst Du für die Verwendung mit Deinen persönlichen Daten. Diese werden gezielt **ausgewertet** und für **Werbung** genutzt. Je nach Deinen Interessen, Alter oder Geschlecht werden dann möglichst passende Werbeinhalte eingeblendet. So wird wahrscheinlicher, dass Du die Werbung anklickst oder diese Wirkung zeigt.

Achtung: Manchmal kann ein Klick auf Werbung zu problematischen Inhalten oder Abzockseiten führen. Sei wachsam und gebe nicht vorschnell private Daten ein.

Mehr Infos gibt es unter www.datenparty.de und www.klicksafe.de/irights im Text 26 „Datenschutz auf Facebook: Wem gehören meine Daten?“

11 Vor Datenmissbrauch ist niemand geschützt

Wenn Du im Internet unerwünschte Daten, Infos oder Bilder von Dir findest, dann gehe dagegen vor. Sage auch Deinen Eltern oder älteren Geschwistern Bescheid, damit sie Dir helfen können. Als Beweis solltet Ihr einen Screenshot von der Internetseite machen.

- Wisst Ihr, wer die Inhalte veröffentlicht hat? Dann fordert die Person schriftlich dazu auf, die Inhalte bis zu einer von Euch festgelegten Frist zu entfernen. Die Frist sollte nicht zu kurz sein, damit der oder die Betroffene Zeit hat zu reagieren.
- Wenn dies nichts bringt oder nicht möglich ist, informiert den Betreiber der Seite und bittet um Löschung. Auch hier sollte eine Frist genannt werden. Ihr findet die Kontaktdaten im Impressum der Internetseite oder über www.whois.net und www.denic.de. In Sozialen Netzwerken gibt es spezielle Melde-Buttons.
- In schlimmen Fällen (schwere Beleidigungen, problematische Bilder, die schnell entfernt werden sollen) oder wenn die Entfernung nicht klappt, könnt Ihr auch die Polizei oder einen Anwalt einschalten.

Sage Deinen Freunden und Bekannten Bescheid, wenn Du im Internet komische oder peinliche Fotos und andere Infos von ihnen findest.

Inhalte, die über Handy und Apps versendet werden, befinden sich nicht mehr „nur“ auf der jeweiligen Webseite – sie befinden sich auf allen angeschriebenen Geräten. Ein vollständiges Löschen ist so noch schwieriger als im Internet und meist sogar unmöglich. (Obwohl auch im Internet Inhalte vor dem Löschen kopiert und an anderer Stelle immer wieder hochgeladen werden können.) Betroffene müssen vielfach damit leben, dass die Inhalte nie mehr ganz verschwinden. Hier ist die Unterstützung durch Familie, Freunde und Mitschüler umso wichtiger!

12

Sicherheitstipps – So schützt Du Deine Daten

- Benutze **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 Deines Haustieres oder Dein Spitzname). Passwörter sollten zudem regelmäßig geändert werden.
- Passwörter sind Dein **Geheimnis**. So verhinderst Du, dass Fremde auf wichtige Daten zugreifen können.
- Installiere ein **Anti-Virenprogramm** auf Computer und Smartphone und aktualisiere es regelmäßig.
- Schütze Deinen Computer mit einer **Firewall** („Brandwand"). Diese schützt vor unberechtigten Zugriffen aus dem Internet und sollte nie ausgeschaltet werden.
- Sichere Dein **WLAN** zu Hause über eine verschlüsselte Verbindung (am besten WPA2). Wenn Du unterwegs mit Deinem Handy in fremden WLANs surfst, verschicke keine wichtigen Daten.
- Schalte **WLAN** und **Bluetooth** aus, wenn Du sie nicht brauchst.
- Führe regelmäßig **Sicherheits-Updates** („Aktualisierungen") auf Computer und Handy durch. So werden Sicherheitslücken geschlossen. Prüfe vor App-Aktualisierungen, ob Zugriffsrechte unnötig erweitert werden. Anders als beim Betriebssystem sollten Apps deshalb nicht automatisch aktualisiert werden.

- Öffne keine E-Mails oder Nachrichten mit **unbekanntem** Absender, vor allem keine Datei-Anhänge.
- **Antworte nicht** auf unerwünschte E-Mails oder Nachrichten. Weitere nervige Kontaktversuche wären die Folge! Ob bei E-Mails oder Sofortnachrichten – besser ist es, den Absender zu blockieren.
- Am besten legst Du Dir zwei verschiedene **E-Mail-Adressen** zu. Eine gibst Du nur an gute Freunde und Bekannte weiter. Die andere verwendest Du für Anmeldungen, Online-Shopping und so weiter.

www.handysektor.de: Infos zum Thema „Sicherheit in mobilen Netzen"
www.klicksafe.de: Unter „Themen – Datenschutz – Privatsphäre" findest Du weitere passende Infos.

Bist Du ein Datenprofi im Internet?

Nimm die Herausforderung an und mach das Datenschutz-Quiz zum Flyer unter www.klicksafe.de/quiz.

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

LMK Landeszentrale für Medien und Kommunikation

Landeszentrale für (LMK) Rheinland-Pfalz
www.lmk-online.de

lfm: Landesanstalt für Medien Nordrhein-Westfalen (LfM)

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

Es wird darauf hingewiesen, dass alle Angaben in diesen Tipps trotz sorgfältiger Bearbeitung ohne Gewähr erfolgen und eine Haftung des Herausgebers ausgeschlossen ist.

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 gefördert von der Europäischen Union

- Vollständig aktualisierte Auflage 2015 -