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

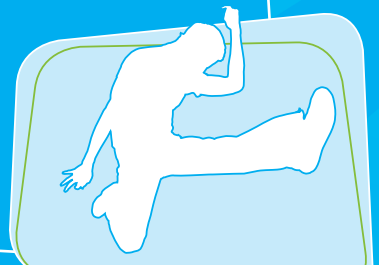
für Eltern

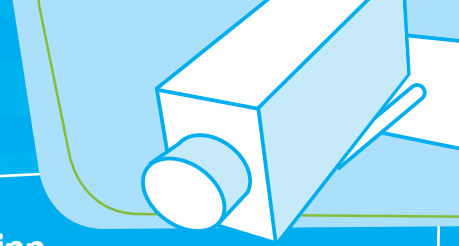
Liebe Eltern!
WhatsApp, Facebook oder Instagram sind bei Jugendlichen – aber auch schon bei einigen Kindern – überaus beliebt. Wer hier nicht mit dabei ist, bekommt vieles nicht oder zu spät mit. Zudem ist spannend zu sehen, wie andere auf eigene Inhalte reagieren. Entsprechend offenherzig gibt man sich in vielen Fällen. Gut gemeinte Ratschläge wie „Verrate nicht zu viel von dir, das Internet vergisst nie!“ stoßen auf Unverständnis: Man tauscht sich doch nur mit Freunden aus und hat ja nichts zu verbergen. Und so glauben viele Kinder und Jugendliche, Datenschutz sei langweilig und gehe sie nichts an.

Aber auch Erwachsene sind im Umgang mit persönlichen Daten nicht immer das beste Vorbild. Dabei ist es im Zeitalter von Smartphones, Onlinebanking, Onlineshopping und großen Datenschutzskandalen wichtiger denn je, persönliche Informationen und Inhalte nicht leichtfertig zu verbreiten.

Dieser Flyer will Ihrer Familie dabei helfen, persönliche Daten bestmöglich zu schützen und das Thema „Datenschutz“ altersgerecht mit Ihrem Kind zu besprechen.

Ihr klicksafe-Team





1 Datenschutz macht Sinn

Informationen wie Name, Adresse oder Telefonnummer nennt man auch **personenbezogene Daten**. Sie verraten viel über die eigene Person und bedeuten für Firmen bares Geld (siehe auch Punkt 5). Aber auch Betrüger versuchen im Internet an sensible Daten zu gelangen, um sie für ihre Zwecke zu missbrauchen.

Grundsätzlich gilt: Je mehr man über das Internet von sich verrät, desto angreifbarer wird man. Denn man weiß nie, was andere mit den Inhalten machen. Und einmal versendet, hat man die Kontrolle über sie verloren. Vor allem sehr persönliche Inhalte will wohl niemand offen im Internet oder auf fremden Handys sehen.

Aber auch eher harmlose Inhalte können schützenswert sein. Denn im Internet ist es leicht möglich, die an verschiedenen Stellen gespeicherten Daten zu verknüpfen. So ergibt sich ein immer genaueres Bild der eigenen Person. Datenschutz und Datensparsamkeit machen also Sinn. Dies sollte auch jüngeren Internet- und Handynutzern klar sein!

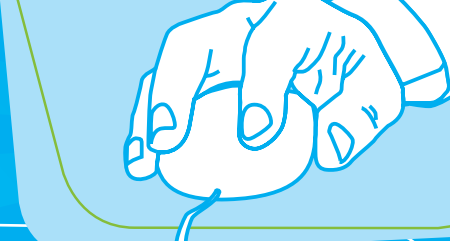
2 Datenschutz ist Ihr gutes Recht

Durch das **Recht auf informationelle Selbstbestimmung** sind personenbezogene Daten in Deutschland sogar per Gesetz geschützt. Niemand darf diese ohne Einwilligung der betroffenen Person speichern, veröffentlichen oder weitergeben. Eine Einwilligung kann z. B. durch Zustimmung zu den **allgemeinen Geschäftsbedingungen (AGB)** eines Angebots während der Anmeldung erfolgen (siehe Punkt 6).

Bei Fotos und Filmen gilt das **Recht am eigenen Bild**: Ausschließlich die abgebildete Person darf entscheiden, welche Aufnahmen von ihr veröffentlicht oder verbreitet werden. Ausnahmen gibt es u. a. für Aufnahmen, auf denen man Teil einer Menschenmenge oder nur „Beiwerk“ ist. (Beispiel: Jemand fotografiert den Kölner Dom und Sie sind zufällig im Bild.)

Übrigens: Bei Kindern bis sieben Jahren sind die Erziehungsberechtigten allein entscheidungsfähig. Von acht bis einschließlich 17 Jahren kommt es nach Meinung vieler Juristen auf den Entwicklungsstand des Kindes an. Bei entsprechender Reife und Einsichtsfähigkeit muss das Kind einer Veröffentlichung ebenfalls zustimmen (Doppelzuständigkeit).

Da der Alltag häufig anders aussieht, geben wir folgende **Tipps**: Tauschen Sie sich regelmäßig mit Ihrem Kind über veröffentlichte und verschickte Inhalte aus. Veröffentlichen Sie keine Baby- oder Kinderfotos/filme – Ihr Nachwuchs wird es Ihnen danken! Versteht Ihr Kind die Folgen, fragen Sie es, **bevor** Sie Aufnahmen Ihres Kindes verbreiten.



3 Jeder hat ein Recht auf Datenschutz

Ihr Kind sollte nicht nur die eigenen, sondern auch die Rechte anderer beachten. Denn: Jeder hat ein Recht am eigenen Wort und am eigenen Bild. Absolut verboten ist es, falsche Daten über jemanden zu verbreiten. Das wäre Rufschädigung und kann strafbar sein.

Tipp für Ihr Kind: Beachte auch die Rechte anderer! Also keine Bilder, Filme oder private Infos von anderen ins Netz stellen oder mit Apps verschicken – außer du hast ihre Erlaubnis. Und selbst wenn du dies einmal vergisst, frage dich **vor** dem Versenden: Wie fändest du es, wenn andere solche Inhalte von dir verbreiten? Wie würde es dir dabei gehen? Könnte der Inhalt von anderen missverstanden werden? Wenn du nicht sicher bist, lass es lieber.

Unter www.klicksafe.de/irights und www.irights.info finden Sie weitere Infos zu Persönlichkeitsrechten und anderen Rechten in der digitalen Welt.

www.handysektor.de: Im Bereich „Datenschutz + Recht “ gibt es passende Inhalte für Jugendliche.

4 Elektronische Datenspuren hinterlässt man auch unbemerkt

Jeder Internet- und Handynutzer hinterlässt Datenspuren – vielfach auch unbemerkt. Auch dies sollten Sie mit Ihrem Kind besprechen. **Zwei Beispiele:**

- Viele vor allem kostenlose **Handy-Apps** greifen auf persönliche Daten wie die Kontakte oder den aktuellen Standort zu – auch wenn dies für die Funktionen der App nicht notwendig ist. App-Berechtigungen sollten deshalb genau geprüft werden (siehe auch Punkt 11).
- Auch **Betriebssysteme** von Tablets, Smartphones oder Computern können sehr „datenhungrig“ sein. Hier sollte man nicht vorschnell allen Standard-einstellungen zustimmen und sich genau informieren: Welche Daten werden an den Anbieter übertragen? Mit welchen Einstellungen können Datenflüsse eingedämmt werden? Wie sieht die Datenschutzerklärung aus?...

Mehr Infos gibt es im Elternratgeber zu Handys, Apps und mobilen Netzen „Smart mobil?!“ und in der Download-Broschüre „Datenschutz im (mobilen) Internet“: www.klicksafe.de/materialien.

5 Umsonst ist nicht kostenlos

Viele Apps, Suchmaschinen oder Soziale Netzwerke sind auf den ersten Blick kostenlos. Tatsächlich funktioniert das Geschäftsmodell so, dass die gespeicherten, eingegebenen oder versendeten Daten ausgewertet und für Werbung genutzt werden. **Zwei Beispiele** von vielen:

- Ihr Kind besucht die Seite eines Prominenten und sieht später dazu passende Werbung. Dies kann an **Cookies** („Kekse“) liegen – kleine Dateien, die automatisch beim Surfen auf dem Computer gespeichert werden. So können Unternehmen die Internetnutzung beobachten und die Interessen der Nutzer herausfinden (siehe auch Punkt 11).
- Einige **E-Mail-Anbieter** „lesen“ die Inhalte von E-Mails automatisch nach Schlüsselwörtern aus, um dem Nutzer dazu passende Werbung zu senden (siehe auch Punkt 11).

Tipp: Sprechen Sie mit Ihrem Kind über Onlinewerbung und das Geschäftsmodell „Bezahlen mit Daten“. 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 unter www.kinder-onlinewerbung.de.
Zum Thema „Abzocke im Internet“ hat klicksafe einen Flyer im Angebot: www.klicksafe.de/materialien.

6 AGB und Co. – Was der Anbieter mit den Nutzerdaten machen darf

Die meisten Webseiten und Apps – vor allem solche, die kommerziell sind, Nutzerdaten abfragen oder Werbung zeigen – verfügen über Allgemeine Geschäftsbedingungen (kurz **AGB**), **Nutzungsbedingungen** und ggf. eine **Datenschutzerklärung**. In dieser erfährt man, was mit den Nutzerdaten passiert, was gespeichert, weitergegeben oder für Werbung genutzt wird. Und mit einer Anmeldung stimmt man diesen Richtlinien automatisch zu!

Nicht nur Kindern und Jugendlichen fällt es häufig schwer, diese sehr juristischen Texte zu lesen und zu verstehen. Entsprechend häufig werden diese ungelesen akzeptiert. Trotzdem lohnt es sich, hier genauer hinzuschauen.

Tipp: Verabreden Sie mit Ihrem (jüngeren) Kind, dass Sie neue Internetangebote oder Apps vorab gemeinsam anschauen und prüfen (siehe Punkt 11). 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.

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/Geburtsjahr enthält, hilft wenig. Ihr Kind kann diesen zum Beispiel in Chats, Foren oder Messengern benutzen.

Tipp für Ihr Kind: Verstecke Dich nicht hinter einem Nickname, um andere zu beleidigen. Dies könnte sogar strafbar sein.

8 „Onlineruf“ regelmäßig prüfen

Je mehr persönliche Daten Ihr Kind im Internet veröffentlicht oder per Handy verschickt, umso weniger können diese kontrolliert werden. Häufig verbreiten aber auch andere private Informationen oder Fotos Ihrer Familie. Deshalb sollte der eigene „**Onlineruf**“ regelmäßig in verschiedenen Suchmaschinen geprüft werden. In Sozialen Netzwerken sollte man Profile von Bekannten nach entsprechenden Inhalten durchsuchen und ggf. um Entfernung bitten.

Tipp: Bei Facebook kann mit der Funktion „Anzeigen aus der Sicht von ...“ überprüft werden, wie die eigene Chronik für die Öffentlichkeit oder für bestimmte Kontakte/Personen aussieht.

9 So wird Ihr Kind ein Datenprofi: Erst denken, dann senden!

Besprechen Sie mit Ihrem Kind, warum persönliche Daten schützenswert sind und seien Sie ein gutes **Vorbild** (siehe auch Punkt 2). Ansonsten werden die besten Datenschutz-Tipps kaum Wirkung zeigen. Prüfen Sie, ob Ihr Kind schon genug Erfahrung hat, um Messenger oder Soziale Netzwerke zu nutzen und achten Sie auf das Mindestalter des Angebots. Vereinbaren Sie, welche Inhalte im Internet ohne Probleme weitergegeben werden können – und welche eher privat bleiben sollten.

Denn Datenschutz heißt nicht, keine persönlichen Inhalte zu teilen. Entscheidend ist die **richtige Auswahl**. Die folgenden **Tipps** können Ihrem Kind bei der Entscheidung helfen:

- Einmal versendete Inhalte können immer wieder im Internet oder auf Smartphones auftauchen. Überlege deshalb **vor dem Absenden**: Wie willst du dich anderen (im schlimmsten Fall) für immer zeigen? Dabei kann dir die **Oma-Regel** helfen, nach dem Motto: Würde ich dies meiner Oma sagen oder zeigen?
- Ein Foto darf ruhig auch mal lustig sein. Allzu **peinliche**, **freizügige** oder **beleidigende** Fotos haben im Internet aber nichts zu suchen. Dies gilt auch für **extreme** oder **verletzende Kommentare**. Und: Je auffallender ein Inhalt ist, desto eher wird er an andere weitergeleitet.
- 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 **Daten**: Lass Anschrift, Handynummer oder E-Mail-Adresse weg und gebe sie nicht leichtfertig an andere weiter.
- Überprüfe regelmäßig deine **Privatsphäre-Einstellungen**. Wenn du etwas nicht verstehst, frage deine Eltern oder ältere Geschwister.
- Auch strenge Privatsphäre-Einstellungen schützen nicht davor, dass **berechtigte Kontakte** Daten oder Fotos kopieren oder weiterleiten. Prüfe deshalb genau, wem du Zugang gibst und was du veröffentlichst. Zudem „liest“ der **Anbieter** vielfach mit und wertet deine Daten aus.
- Nutzt du Soziale Netzwerke oder Messenger mit deinem **Handy**? Dann achte darauf, Bilder, Videos und Infos nicht vorschnell aus der Situation heraus zu verbreiten. Dies gilt besonders für Angebote, die in Echtzeit senden (wie YouNow).

- www.mediennutzungsvertrag.de: Hier können Sie mit Ihrem Kind Regeln für die Mediennutzung in einem gemeinsamen Vertrag festlegen.
- Tipps zu Messengern und Sozialen Netzwerken gibt es im klicksafe-Flyer „Sicherer in Sozialen Netzwerken: Tipps für Eltern“: www.klicksafe.de/materialien.

10 Tipps: Richtig reagieren bei Datenmissbrauch

Verbreiten sich unerwünschte persönliche Daten, Infos oder Bilder im Internet oder auf fremden Handys, 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 seltsame 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 darüber hinaus auch auf allen angeschriebenen Geräten. Ein vollständiges Löschen ist so noch schwieriger und meist sogar unmöglich. Betroffene müssen vielfach damit leben. Hier ist die soziale Unterstützung durch Familie, Freunde und Mitschüler umso wichtiger! Wenn unerwünschte Inhalte Ihres 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.

Weitere Informationen gibt es unter www.klicksafe.de/irights (u. a. in den Schwerpunkten 1 und 8) sowie in der klicksafe-Broschüre „Ratgeber Cyber-Mobbing“ unter www.klicksafe.de/materialien.

11 Sicherheitstipps – So sind die Daten Ihrer Familie gesichert

- Benutzen Sie **sichere Passwörter** und nicht immer dasselbe. Passwörter sollten nicht leicht zu erraten sein sowie regelmäßig **geändert** und **nicht weitergegeben** werden (siehe auch www.klicksafe.de/sicheres-passwort).
- Sichern Sie mobile Geräte mit **PIN** oder **Passwort**.
- **Loggen Sie sich aus**, bevor Sie Webseiten mit Login-Funktion verlassen – besonders auf fremden Computern.
- Nutzen Sie ein **Anti-Virenprogramm** auf Computer und Smartphone und aktualisieren Sie es regelmäßig.
- Schützen Sie Ihren Computer mit einer **Firewall**.
- **Verschlüsseln** Sie wichtige Daten, E-Mails, USB-Sticks und andere mobile Datenträger.
- Sichern Sie Ihr **WLAN-Netzwerk** über eine verschlüsselte Verbindung (möglichst WPA2). In fremden WLANs sollten keine wichtigen Daten verschickt werden (Onlinebanking, Kreditkarten-Nummer, ...).
- Schalten Sie **WLAN, GPS & Bluetooth** aus, wenn sie nicht benötigt werden.
- Prüfen Sie neue Apps und die Verhältnismäßigkeit der eingeforderten Berechtigungen vor der Installation. Schauen Sie sich die Bewertungen und Kommentare anderer Nutzer an. Hier kann auch der **App-Check** von klicksafe und Handysektor helfen: www.klicksafe.de/apps.
- Führen Sie regelmäßig **Sicherheits-Updates** von Betriebssystem, Programmen und Apps durch. So werden Sicherheitslücken geschlossen. Prüfen Sie bei App-Updates, ob Berechtigungen unnötig erweitert werden.
- Stellen Sie Ihr **Betriebssystem** so ein, dass möglichst wenig Daten an den Hersteller gesendet werden (siehe auch Punkt 4).
- Auf **unerwünschte** E-Mails oder Nachrichten mit **unbekanntem** Absender sollte nicht geantwortet werden. Zudem sollten keine mitgeschickten Dateien oder Links angeklickt werden. Besser ist es, den Absender zu blockieren.
- Nutzen Sie die Privatsphäre-Einstellungen von „**Kommunikations-Apps**“. Prüfen Sie, ob diese Ihre Daten verschlüsselt versenden (am besten mit Ende-zu-Ende-Verschlüsselung).
- Prüfen Sie, auf welche Daten Ihr **E-Mail-Dienst** zugreift und ob die Server des Anbieters in Deutschland oder im Ausland stehen. Ggf. kann im Sinne des Datenschutzes auch ein kostenpflichtiger Dienst sinnvoll sein.
- Nutzen Sie nicht zu viele Dienste von **ein und demselben Anbieter** – Ihre Daten können sonst leicht verknüpft werden.
- Probieren Sie **alternative Suchmaschinen** wie DuckDuckGo, Ixquick oder Startpage aus.
- Deaktivieren Sie **Drittanbieter-Cookies** in Ihrem Browser und löschen Sie Cookies regelmäßig.

Bist Du ein Datenprofi im Internet?
Spielen Sie das Quiz gemeinsam mit Ihrem Kind, um über Datenschutz ins Gespräch zu kommen:
www.klicksafe.de/quiz.

klicksafe ist das deutsche Awareness Centre im CEF Telecom Programm 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: © momius – 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

- 5. vollständig aktualisierte Auflage Mai 2016 -