klicksafe

Datenschutz

So sind persönliche Daten im Internet sicherer

Tipps für Eltern

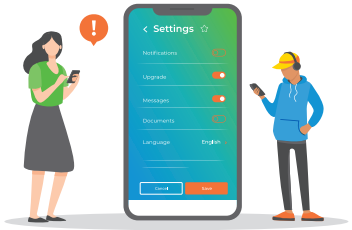
In Zusammenarbeit mit:

LDI NRW
Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen

Datenschutz-Tipps
für Eltern

WhatsApp, Instagram oder YouTube 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.



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 Geräten 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.

Mehr Infos zu den Themen Datenschutz und Privatsphäre finden sich unter www.klicksafe.de/privatsphaere-und-big-data.

2 Datenschutz ist Ihr gutes Recht

Personenbezogene Daten sind in der Europäischen Union und damit auch in Deutschland durch die **Datenschutz-Grundverordnung (DSGVO)** geschützt. Niemand darf diese Daten ohne eine Rechtsgrundlage, z. B. einer Einwilligung der betroffenen Person, speichern, veröffentlichen oder weitergeben. Eine Einwilligung kann auf einer Website z. B. durch ein Pop-up eingeholt werden.

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. Übrigens: Bei Kindern bis 16 Jahre müssen laut DSGVO die Eltern die Einwilligung erteilen. Ab einem Alter von 16 Jahren können Jugendliche selbst entscheiden.

Tipp: 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.

Weitere Infos zur Datenschutz-Grundverordnung finden Sie unter deinedatendeinerechte.de.

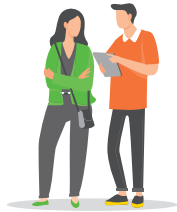
3 Jeder hat ein Recht auf Datenschutz

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?

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

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



4 Digitale Datenspuren hinterlässt man auch unbemerkt

Jede Internetnutzerin und jeder Internetnutzer **hinterlässt Datenspuren** – vielfach auch unbemerkt. Auch dies sollten Sie mit Ihrem Kind besprechen. Drei Beispiele:

- Viele vor allem kostenlose **Smartphone-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.
- Auch **Betriebssysteme** von Tablets, Smartphones oder Computern können sehr „datenhungrig“ sein. Hier sollte man nicht vorschnell allen Standardeinstellungen zustimmen und sich genau informieren.
- Auch die neuen **digitalen und vernetzten Gegenstände** (z. B. Smart Speaker, Smart Home) können private Daten aus unserem persönlichen Lebensumfeld aufzeichnen und verarbeiten.

Mehr Infos zu Smartphones, Apps und mobilen Netzen gibt es im Elternratgeber „Smart mobil?!: www.klicksafe.de/materialien.

Im klicksafe-Themenbereich „Smartes Leben“ finden Sie Tipps zum sicheren Umgang mit smarten Technologien: www.klicksafe.de/smart-home.

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 Herstellers für Sportbekleidung und sieht später dazu passende Werbung. Dies kann an **Cookies** liegen – kleine Dateien, die automatisch beim Surfen auf dem Gerät gespeichert werden. So können Unternehmen die Internetnutzung beobachten und die Interessen der Nutzerinnen und Nutzer herausfinden.
- Einige **E-Mail-Anbieter** „lesen" die Inhalte von E-Mails automatisch nach Schlüsselwörtern aus, um Nutzerinnen und Nutzern dazu passende Werbung zu senden.

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 Abzockeseiten führen kann.

Weitere Infos zum Thema Onlinewerbung gibt es in der klicksafe-Broschüre „Werbung und Kommerz im Internet" (www.klicksafe.de/materialien) und www.kinder-onlinewerbung.de.

6 Was der Anbieter mit den Nutzerdaten machen darf

Websites und Apps müssen eine **Datenschutzerklärung** enthalten, die für jeden leicht zugänglich und verständlich ist. Hierin erfährt man, was mit den Daten der Nutzerinnen und Nutzer passiert, was gespeichert, weitergegeben oder für Werbung genutzt wird. Bei der Weitergabe der personenbezogenen Daten an Dritte muss eine Einwilligung der Nutzerinnen und Nutzer eingeholt werden.

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. Im Zweifel sollte Ihr Kind lieber auf eine Nutzung verzichten – auch wenn es häufig schwerfällt.

Die von klicksafe zusammengefassten Nutzungsbedingungen für beliebte Dienste finden Sie unter: www.handysektor.de/mediathek/nutzungsbedingungen-kurzgefasst.

7 Pseudonym nutzen, unerkannt surfen

Ein **gutes Pseudonym** („Deckname“) kann dabei helfen, im Internet unerkannt zu surfen. Ihr Kind kann dieses zum Beispiel in Chats, Foren oder Messengern benutzen. Hierbei ist Erfindungsgeist gefragt. Ein Deckname, der dem richtigen Namen zu ähnlich ist oder das Alter/Geburtsjahr enthält, hilft wenig.

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

8 „Onlineruf“ regelmäßig prüfen

Je mehr persönliche Daten Ihr Kind im Internet veröffentlicht oder per Smartphone verschickt, umso weniger können diese kontrolliert werden. Häufig verbreiten sich aber auch andere private Informationen oder Fotos Ihrer Familie.

Deshalb sollte der eigene **„Onlineruf“ (Onlinereputation)** regelmäßig in verschiedenen Suchmaschinen geprüft werden. In Sozialen Netzwerken sollte man Profile von Bekannten nach entsprechenden Inhalten durchsuchen und ggf. um Entfernung bitten.

Schon gewusst?

Unter www.fragzebra.de können Sie alle Fragen zum digitalen Alltag stellen – ein Team aus Expertinnen und Experten der Landesanstalt für Medien NRW beantwortet diese kostenlos, anonym und individuell.

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?
- Ein Foto oder Video darf ruhig auch mal lustig sein. Allzu **peinliche**, **freizügige oder beleidigende** Fotos und Videos haben im Internet aber nichts zu suchen. Dies gilt auch für extreme oder verletzende **Kommentare**.
- 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 Smartphone? Dann achte darauf, Bilder, Videos und Infos **nicht vorschnell** und leichtsinnig aus der Situation heraus zu **verbreiten**. Dies gilt besonders für Angebote, die **in Echtzeit** senden oder bei denen der hochgeladene Inhalt nur für eine begrenzte Zeit gesehen werden kann (z. B. Snapchat, Instagram-Stories), denn auch hier gibt es technische Möglichkeiten Bilder zu speichern und weiterzuverbreiten.

Unter www.mediennutzungsvertrag.de 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 Diensten – Tipps für Eltern“: www.klicksafe.de/materialien.

Eltern finden auf der klicksafe-Website weitere Infos zum sicheren Umgang mit dem Internet und Sozialen Netzwerken: www.klicksafe.de/bildschirm-und-medienzeit-was-ist-fuer-kinder-in-ordnung.

10 Richtig reagieren bei Datenmissbrauch

Verbreiten sich unerwünschte persönliche Daten, Infos oder Bilder im Internet oder auf fremden Smartphones, dann **gehen Sie dagegen vor**. Nach der DSGVO haben die Betroffenen ein Recht gegenüber dem Verantwortlichen darauf, dass die personenbezogenen Daten gelöscht werden. 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 keine Wirkung zeigt oder nicht möglich ist, wenden Sie sich an den **Betreiber der Internetseite**. Setzen Sie auch hier eine Frist. In Sozialen Netzwerken gibt es spezielle Melde-Buttons.
- Ist auch dies erfolglos, können Sie sich an die **Datenschutzaufsichtsbehörde** Ihres Bundeslandes oder bei Bedarf an einen Anwalt wenden.
- 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 Smartphones 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 Mitschülerinnen und Mitschüler umso wichtiger! Wenn unerwünschte Inhalte Ihres Kindes auf Smartphones 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 in der klicksafe-Broschüre „Ratgeber Cyber-Mobbing“ unter www.klicksafe.de/materialien.

www.klicksafe.de/quiz Spielen Sie das **Datenschutz-Quiz** für Jugendliche gemeinsam mit Ihrem Kind, um über den sicheren Umgang mit Daten ins Gespräch zu kommen.

www.klicksafe.de/checklisten Mithilfe der **Datenschutz-Checkliste** können die Daten Ihrer Familie gesichert werden.

klicksafe ist Koordinator des deutschen Safer Internet Centres der Europäischen Union.

klicksafe sind:

Medienanstalt Rheinland-Pfalz

Medienanstalt Rheinland-Pfalz
www.medienanstalt-rlp.de

LANDESANSTALT FÜR MEDIEN NRW
Der Meinungsfreiheit verpflichtet.

Landesanstalt für Medien NRW
www.medienanstalt-nrw.de

Kofinanziert von der Europäischen Union

7. Auflage, Oktober 2022

Herausgeber:

klicksafe
c/o Landesanstalt für Medien NRW
Zollhof 2
40221 Düsseldorf

T +49 (0)211-77 00 7-0
F +49 (0)211-72 71 70

klicksafe@medienanstalt-nrw.de
www.klicksafe.de