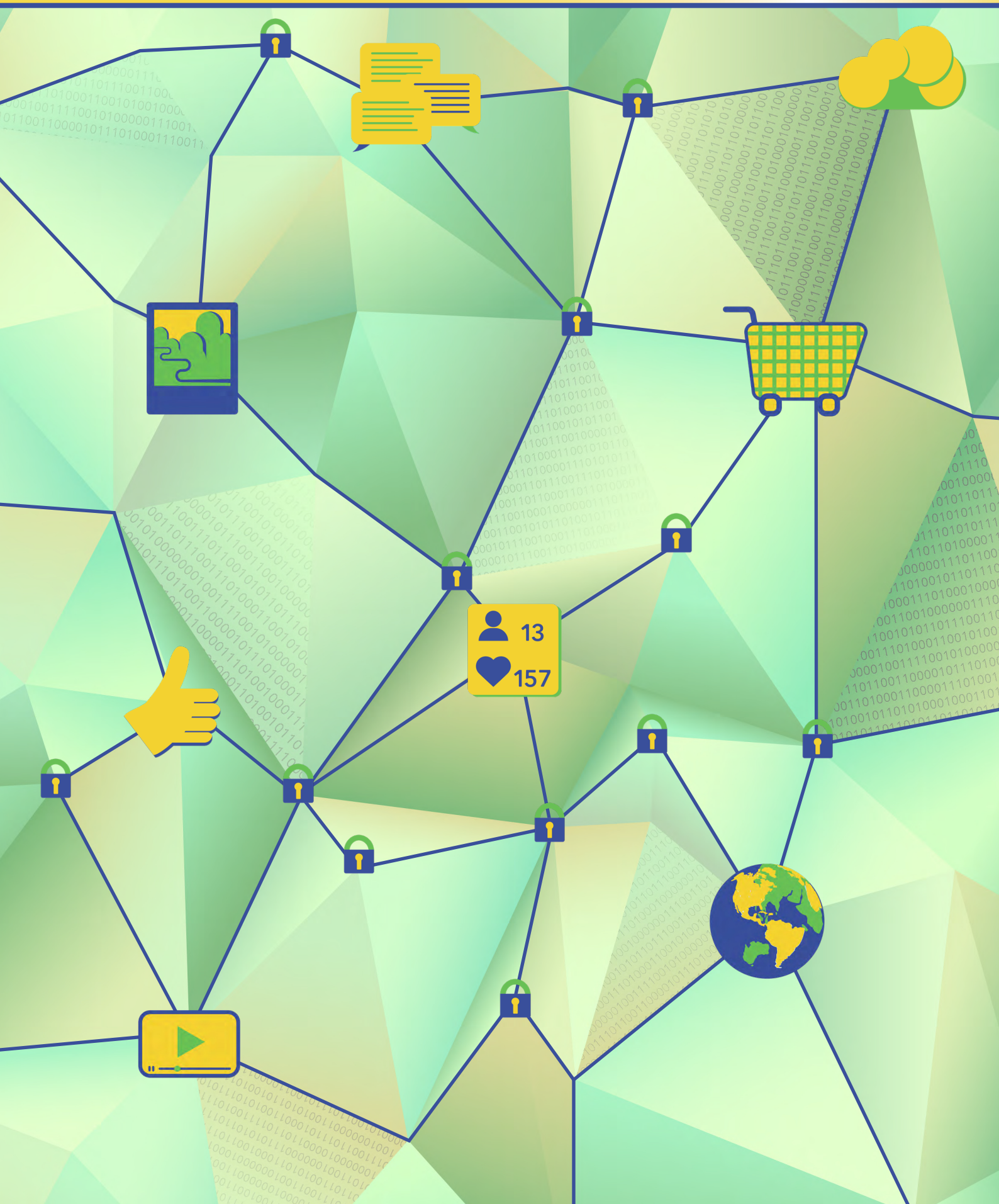
Datenschutz in sozialen Netzwerken: Sehen und gesehen werden



KURZ und KNAPP

Grundsätzlich sind **Social-Media-Plattformen und Datenschutz** nur schwer vereinbar: Das sogenannte **„Privatsphäre-Dilemma“** resultiert daraus, dass **Facebook und Co.** stets ein Stück weit der **extrovertierten Selbstdarstellung** dienen.

Die **Privatsphäre-Einstellungen** sind das A und O um **den Datenschutz bei sozialen Netzwerken** so gut wie möglich zu gewährleisten. Nehmen Sie sich die Zeit, diese zu **prüfen** und **sorgfältig einzustellen**.

Es geht nicht nur um **Ihren eigenen Datenschutz**: In sozialen Netzwerken müssen Sie auch die Rechte **anderer Mitglieder** achten – etwa das **Recht am eigenen Bild**.

Beim **Social-Media-Monitoring** ist in Sachen Datenschutz einiges zu beachten: Personenbezogene Daten dürfen nur dann **erhoben, gespeichert und verwendet** werden, wenn deren Besitzer darin **eingewilligt** hat oder wenn sie **öffentlich zugänglich** sind. Im Zweifelsfalle ist eine **Anonymisierung** vorzunehmen.

INHALT

DATENSICHERHEIT und DATENSCHUTZ in sozialen Netzwerken: Tipps für Nutzer

Datenschutz und Social Media: Ist das nicht ein **Widerspruch** in sich? In der Tat stehen sich die **Grundprinzipien** beider Konzepte gegenseitig **meist im Weg**. Der **Grundsatz** „Teile nur, was auch noch in zehn Jahren über dich im Internet finden möchtest“ reicht nämlich **nur bedingt** aus, um soziale Netzwerke in Sachen Datenschutz im Internet **sicher zu nutzen**.

Folgender **Ratgeber** erläutert, welche Maßnahmen sinnvoll sind. Eines ist jedoch vorab klar: Möchten Sie einen gewissen **Datenschutz-Standard** in sozialen Netzwerken erreichen, sind **Selbstdisziplin und Zeitinvestment** notwendig.

Das Internet vergisst nichts…

2017

2027

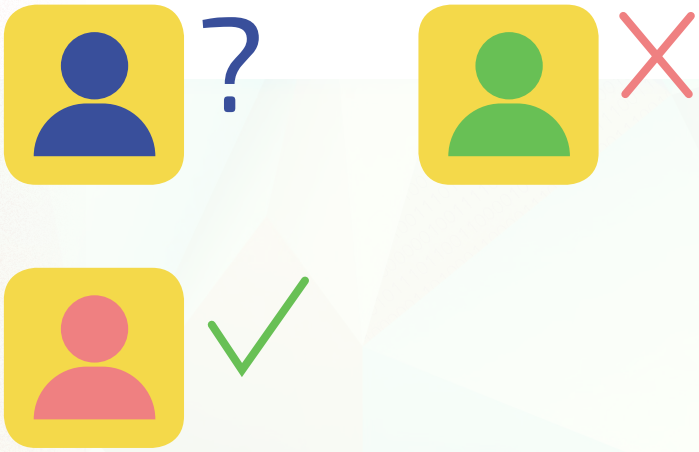
Vor der ANMELDUNG: Grundsätzliche Überlegungen

Bevor Sie sich in einem **sozialen Netzwerk anmelden**, sollten Sie festlegen, welche **Erwartungen** Sie an der Teilnahme am Netz haben. Sollen Ihre **Freunde** Sie finden können? Möchten Sie auch zu **Fremden** Kontakt?

Oftmals können Sie durch einen **sorgfältigen Anmeldeprozess** eventuelle Datenschutzprobleme von vorneherein **ausschließen**. Daher empfiehlt es sich:

- für jedes Netzwerk eine **separate E-Mail-Adresse** zu verwenden. Dies stellt einerseits einen größeren **Aufwand** dar, schützt aber Ihre **Privatsphäre** signifikant.
- genau zu überlegen, ob Sie mit Ihrem **Klarnamen oder einem Pseudonym** auftreten möchten – letzteres ist nur bei **manchen sozialen Netzwerken** pflichtig.
- vorab **festzulegen**, was Sie mit dem Profil bewirken möchten: Soll es ein **rein privates Profil** sein oder ist eine **geschäftliche Nutzung** vorgesehen?

Widerstehen Sie auch der Versuchung, wahllos jedes mögliche Profil als Freund hinzuzufügen.



Privatsphäre-Einstellungen: Bei FACEBOOK, TWITTER und Co. ein MUSS

Umfangreich, nervenaufreibend und zeitfressend: Viele **Social-Media-Nutzer** verzichten auf die Einstellung der **Privatsphäre-Optionen**, weil ihnen dies **zu aufwendig** vorkommt. Doch genau in diesem **Justierungs-Irrgarten** versteckt sich die Möglichkeit, den bestmöglichen Datenschutz in **sozialen Medien** zu gewährleisten.

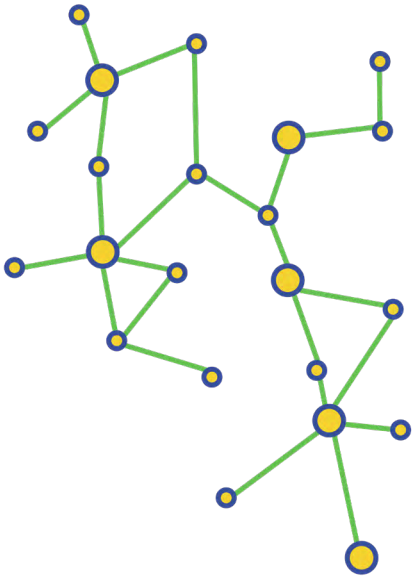
Achten Sie dabei besonders auf **folgende Punkte**:

- **Profil für Suchmaschinen unsichtbar machen**: Diese Option bieten viele Social-Media-Plattformen – allerdings sind die Einstellungen **mitunter versteckt**. Wenden Sie sich ggf. an das **Hilfecenter** des Netzes.

- **Sichtbarkeit von Kontaktdaten**: Sofern Sie das Konto nicht geschäftlich nutzen, sollten Sie Ihre Kontaktdaten **für niemanden sichtbar** machen.

- **Sichtbarkeit Ihrer Inhalte**: Beiträge, Profilbilder, Fotoalben… in den meisten Netzwerken können Sie **genau auswählen**, wer bestimmte Inhalte sehen darf. Hier gilt die Prämisse: **Je weniger, desto besser.**

Auch wenn es mühsam ist: Es lohnt sich, alle Einstellungsoptionen zu prüfen und ggf. anzupassen. Datenkraken setzten in der Regel darauf, dass Nutzer ihre Daten aus Bequemlichkeit nicht schützen.



Kennen Sie Ihre RECHTE – und SETZEN Sie diese durch!

Auch wenn soziale Netzwerke **weltweit agieren** und meist in anderen Ländern basiert sind: Hierzulande müssen sie sich an das **deutsche Recht halten** – also an das Bundesdatenschutzgesetz (BDSG). Dieses besagt **nicht nur**, dass eine **Datenschutzerklärung** vorhanden sein muss, sondern ebenfalls, dass Nutzer der Erhebung ihrer Daten und den AGB **widersprechen** können müssen. Ein solcher Widerspruch resultiert allerdings meist in einer **Löschung des betroffenen Kontos**.

Kaum ein **Rechtsgrundsatz** wird bei Facebook, Twitter und Co. häufiger verletzt als das **Recht am eigenen Bild**. Wurden Fotos von Ihnen **ohne Ihre Zustimmung** veröffentlicht, haben Sie einen Anspruch auf deren **Löschung**. Dies geht aus **§ 22 des Kunsturheberrechtgesetzes (KunstUrhG)** hervor.

Zunächst können Sie die **hochladende Person** mit einem Verweis auf Ihren **Datenschutz** darum bitten, das Bild zu entfernen. Erfolgt innerhalb einer **angemessenen Frist** keine Reaktion, können Sie das Bild **bei dem Betreiber der Plattform melden**.

Erfolgt auch hier keine Reaktion, können Sie einen Anwalt einschalten. Sie haben ein Anrecht darauf, dass Ihr Datenschutz in sozialen Netzwerken im Rahmen des Gesetzes beachtet wird.

Bleiben Sie SOZIAL: Nicht nur Ihre PRIVATSPHÄRE zählt

Bedenken Sie: Nicht nur Sie sind danach bestrebt, Ihren **Datenschutz in sozialen Netzwerken** zu gewährleisten. Aus diesem Grund ist der **Umgang mit fremden Daten** innerhalb des Netzes ebenfalls **wichtig**. Die Plattformen bieten nämlich mehr als eine Möglichkeit, **fremde Daten zu teilen**.

So bieten viele soziale Netzwerke an, nach **möglichen Kontakten** zu suchen – allerdings müssen Sie dafür Ihr **Adressbuch** hochladen. Mit diesem Schritt geben Sie die **E-Mail-Adressen** all Ihrer Kontakte preis.

Auch das Hochladen von **Fotos**, auf denen andere Personen zu sehen sind, sollte **nicht ohne Absprache** erfolgen. Dies gilt auch für das „**Markieren**" von Personen auf Fotos, welches beispielsweise **Facebook** anbietet.

Ebenso sollten Sie der **Bitte**, ein Foto zu **löschen**, auf dem die betroffene Person zu sehen ist, **schnellstmöglich nachkommen.**

Ohne Kontrolle geht es nicht

Alle oben genannten Tipps verhelfen Ihnen zu einem möglichst sicheren Start in sozialen Netzwerken. Allerdings erfordert die Wahrung Ihres Datenschutzes ebenfalls, dass Sie regelmäßig Überprüfungen durchführen.

Checken Sie dabei, ob sich die Privatsphäre-Einstellungen geändert haben, ob Fotos von Ihnen ohne Ihr Wissen hochgeladen wurden und ob sich in Ihrer Freundesliste Profile eingeschlichen haben, die Sie nicht kennen und mit denen Sie keinen Kontakt haben.

Datenschutz beim SOCIAL-MEDIA-MONITORING achten: UNTERNEHMEN müssen vorsichtig sein

Die **Auswertung der Inhalte sozialer Netzwerke** – „Social-Media-Monitoring" – erfährt einen **rasanten Aufschwung**. Trends erkennen, Meinungsführer analysieren und so der Zukunft vorgreifen: Das **neue Geschäftsmodell** verspricht jenen Unternehmen, welche in die Materie eintauchen, einen signifikanten **Marktvorsprung**.
Doch wie sieht es mit dem **Datenschutz** aus, wenn soziale Netzwerke zur **Informationsquelle Nummer 1** werden?

Personenbezogene Daten werden in Deutschland vom Bundesdatenschutzgesetz **besonders geschützt**. Grundsätzlich dürfen diese **Informationen** nur dann erhoben, verarbeitet und gespeichert werden, wenn deren **Besitzer** (also die Person, auf welche sich die Daten beziehen) darin **einwilligt**.
Doch **§ 29 BDSG** bestimmt weiterhin, dass personenbezogene Daten dann **genutzt werden** dürfen, wenn

> [...] die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Speicherung oder Veränderung offensichtlich überwiegt

Unternehmen, welche auf Social-Media-Monitoring setzen, steht eine **weitere Option** zur Verfügung: Sie können auch dann **private personenbezogene Daten** nutzen, wenn sie diese **anonymisieren**.

Diese Regelung erlaubt also die Verwendung all jener Informationen, welche ein Social-Media-Nutzer öffentlich für alle zugänglich macht. An dieser Stelle zeigt sich, wie wichtig sorgfältige Einstellungen sind, um den Datenschutz in sozialen Netzwerken zu gewährleisten.

Impressum

Unter diesem Link gelangen Sie zu unserem Impressum: **Impressum**