# Warum ist Selbstdaten-schutz wichtig?

## Preisgabe von Daten

Viele Angebote im Internet, z. B. Social-Media-Angebote, ermöglichen es, sich selbst darzustellen, mit anderen auszutauschen und sich zu vernetzen. Wer die Angebote nutzen will, gibt persönliche Daten preis. Schon bei der Anmeldung werden viele Daten abgefragt, wie Name, Geburtsdatum, E-Mail und Telefonnummer. Im eigenen Profil möchte man anderen oft möglichst viele verschiedene Dinge von sich und dem eigenen Leben zeigen, um interessant zu wirken. Daher werden oft persönliche Daten preis-gegeben, die man in einem persönlichen Gespräch oder einer anderen Alltagssituation eher nicht gleich erzählen würde, wie Beziehungsstatus, Geschlechterzuordnung, sexuelle oder politische Orientierung oder Religionszugehörigkeit.

## Spannungsfeld: Selbstdarstellung und Datenschutz

Besonders für Kinder und Jugendliche ist es schwierig, ihr Bedürfnis nach Selbstdarstellung und den Schutz der eigenen Privatsphäre unter einen Hut zu bringen.
**Problem:** Es ist ihnen oft nicht bewusst, welche Nachteile es für sie haben kann, wenn Fremde auf ihre Daten zugreifen.

## Persönliche Daten – ein gutes Geschäft

Persönliche Daten sind wie Gold für die Betreiber von Social-Media-Angeboten. Markt-datenhändler, Internet-Tracking-Unternehmen und die Werbewirtschaft freuen sich über wertvolle Daten der einzelnen Nutzerinnen und Nutzer, wie Wohnort, Hobbys, Nutzungsgewohnheiten und vieles mehr. Diese Daten weiter zu verkaufen, ist ein sehr gutes Geschäft. Daher sollte man sich die Datenschutzerklärung und die Allgemeinen Geschäftsbedingungen der Angebote genau anschauen. Besonders die Anbieter vieler Apps von Spielen und Social-Media-Angeboten stehen hier in der Kritik. Dort müssen die Nutzerinnen und Nutzer oft in die Weitergabe ihrer Daten einwilligen, sonst können sie das Angebot nicht nutzen.

## Spam?

Ihr Briefkasten enthält plötzlich viel mehr Werbesendungen oder Ihr E-Mail-Konto wird von Spam-Mails geflutet? Möglicherweise haben Sie Ihre Daten in einem unseriösen Online-Angebot preisgegeben und Ihre Daten wurden weiterverkauft.

## Missbrauch von Daten

Im Internet hinterlässt man – oftmals unbemerkt – viele Spuren, die schwerwiegende Folgen haben können. Daten können durch Fremde missbraucht werden, wenn an einem Profil keine oder zu wenig Privatsphäre-Einstellungen vorgenommen wurden. Persönliche Informationen sind dann öffentlich und können leicht gestohlen und missbraucht werden. Doch auch mit den richtigen Privatsphäre-Einstellungen können Daten gestohlen werden, etwa wenn sich Hacker durch Sicherheitslücken auf der Plattform Zugriff verschaffen.

## Identitätsdiebstahl

Eine besondere Form des Datenmissbrauchs ist der Identitätsdiebstahl. Hier gibt sich eine Person als eine andere aus. Dazu wird oft ein gefälschtes Profil (Fake-Profil) erstellt. Das Fake-Profil soll der eigentlichen Person schaden, z. B. wenn rufschädigende Nachrichten oder Bilder veröffentlicht werden. Oft werden mit dem Fake-Profil auch andere Nutzerinnen und Nutzer kontaktiert. Sie erkennen oft nicht, dass es nicht die richtige Person ist und geben ebenfalls persönliche Daten preis, die dann auch missbraucht werden.

## Konto gehackt?

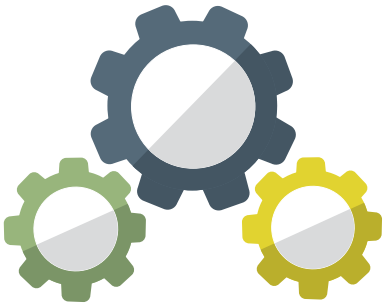
Durch Identitätsdiebstahl kann auch ein finanzieller Schaden entstehen, z. B. wenn Bezahl- oder Kontodaten gestohlen werden und Geld abgebucht wird. Oft reichen schon Name und Adresse eines Opfers aus, um beispielsweise etwas in seinem Namen online zu bestellen. Schauen Sie genau hin, bevor Sie Ihre Konto- oder Kreditkarten-Daten im Internet verwenden und prüfen Sie Ihre Kontoauszüge.

## Sind gelöschte Daten wirklich weg?

Digitale Daten lassen sich sehr schnell weiterleiten, vervielfältigen und verbreiten. Sind sie erstmal online, kann man sie nicht mehr zurückholen: Das Internet vergisst nichts. Online gestellte Daten können auch nach Jahren wieder auftauchen, obwohl man sie eigentlich gelöscht hat. So können dann auch zukünftige Arbeitgeber oder neue Partnerinnen und Partner diese Daten abrufen. Auch wenn man den Datenschutz ernst nimmt, kann man nie sicher sein, dass Fotos und Informationen der eigenen Person nicht trotzdem irgendwo im Internet herumgeistern – z. B. eingestellt durch Freundinnen oder Freunde. Zum Schutz der Privatsphäre sollte man also grundsätzlich sparsam mit seinen Daten sein. Man sollte sich in jeder Situation fragen, was man wirklich von sich preisgeben möchte und ob es notwendig ist.

## Wie lassen sich eigene Daten am besten schützen?

Der beste Schutz von Daten ist es, sie gar nicht erst zu veröffentlichen. Auf jeden Fall sollte man gerade mit persönlichen Daten wie Name, Adresse, Geburtstag oder Telefonnummer sparsam umgehen und sie nicht einfach so herausgeben. Fragt ein Angebot zu viele dieser Daten ab, sollte man sich überlegen, ob man es wirklich nutzen möchte. Manchmal gibt es auch datensparsame Alternativen. Generell gilt: Weniger ist mehr. Daten, die nicht online stehen, können auch nicht so leicht missbraucht werden.



### Tipp

Privatsphäre-Einstellungen sollten unbedingt vorgenommen und regelmäßig überprüft und aktualisiert werden. Eine der wichtigsten Datenschutzfunktionen bei Social-Media-Angeboten ist die Sichtbarkeit. Eigene Daten sollten nicht öffentlich, sondern nur für ausgewählte Kontakte („Freunde“) sichtbar sein. Eine weitere Möglichkeit ist es, Zugriffsrechte von Apps einzuschränken. So kann geprüft werden, auf welche Daten eine App zugreifen kann und ob sie den Zugriff wirklich benötigt.

Weitere Informationen zum Thema Datenschutz sowie konkrete Tipps für technische Einstellungen finden Sie in der Broschüre **„Selbstdatenschutz! Tipps, Tricks und Klicks“** der Bayerischen Landeszentrale für neue Medien (BLM).

**Quellenangabe**

Der Text ist Bestandteil der bereits bestehenden Unterrichtseinheit „Liken, posten, teilen“ des Medienführerscheins Bayern für den Bereich der sonderpädagogischen Förderung. Die Unterrichtseinheit ist verfügbar unter: **www.medienfuehrerschein.bayern.** Die Entwicklung wurde gefördert durch die Bayerische Staatskanzlei.