
# ICH SUCHE DICH.

## Wer bist du?

**Soziale Netzwerke & Datenschutz**
**Tipps für Jugendliche**

jugendnetz-berlin.de

Berliner Beauftragter für Datenschutz und Informationsfreiheit

# Hast du auch ein Profil in einem sozialen Netzwerk wie Facebook, Google+ oder WhatsApp? Was erfährt man über dich? Welche Informationen gibst du preis?

... erfährt man von deinen Hobbys, Lieblingsfilmen und Büchern? ... deiner politischen Einstellung? ... hast du Fotos von dir veröffentlicht? ... schreibst du ein Weblog? ... Und findet man vielleicht sogar deine Kontaktdaten, wo du gerade bist oder was du gerade machst?

Gibst du in der virtuellen und scheinbar anonymen (Online-) Welt Informationen preis, die du im realen Leben vielleicht sogar deinen besten Freunden verschweigen würdest?

Welche Risiken und Gefahren für deine Persönlichkeitsrechte damit verbunden sein können, ist dir vielleicht gar nicht bekannt.

Wir wollen mit unseren Hinweisen aus datenschutzrechtlicher Sicht über mögliche Risiken von sozialen Netzwerken aufklären, damit du keinen Ärger bekommst.

# Das Internet vergisst nichts!

Was du heute lustig findest, ist dir morgen vielleicht richtig peinlich oder unangenehm. Informationen, die du ins Netz gestellt hast, sind jedem zugänglich und sie können unkontrolliert kopiert und in andere Zusammenhänge gebracht werden. Und auch wenn du dir überlegt hast, deine Daten im Netz lieber wieder zu löschen oder zu ändern, gibt es spezielle Dienstleister, die diese Veränderung deiner Daten feststellen können.

Eine Trennung von Schule bzw. Beruf und Privatleben oder auch ein „Vergessen“ von „Jugendsünden“ kannst du im Internet nur dann erfolgreich durchsetzen, wenn du im Internet Spitznamen (Pseudonyme) nutzt, die nur wenigen Eingeweihten (z.B. deinen Freunden) bekannt sind.

Diese Grundregel solltest du bei der Nutzung von sozialen Netzen beachten, da du keine Kontrolle hast, wer sich dein eingestelltes Profil ansieht.

Das Internetarchiv (www.archive.org) hat sich vorgenommen, das gesamte Internet zu archivieren. Von jeder erfassten Webseite sind auf einem Zeitstrahl auch frühere Versionen vorhanden, also vielleicht auch persönliche Daten zu lesen, die eigentlich längst gelöscht sein sollten.

# In welchem Netzwerk bist du richtig?

Es gibt soziale Netzwerke für unterschiedliche Bedürfnisse. Während du die einen für private Zwecke (z. B. Facebook) nutzt, kannst du in anderen Netzwerken berufliche Kontakte (z.B. Xing) knüpfen. Wenn du nur Kontakt mit Freunden halten willst, sind Chatdienste wie WhatsApp, Threema und SnapChat besser geeignet. Sie sind eher ein Ersatz für die SMS als soziale Netzwerke, obwohl auch da persönliche Daten veröffentlicht werden (z. B. Profilbild, Status).

Achte hier auf Ende-zu-Ende-Verschlüsselung und darauf, wer den Dienst betreibt. Europa hat meist ein höheres Datenschutzniveau. Interessant sind auch Dienste, die Nachrichten nach einiger Zeit automatisch löschen – verlasse dich aber nicht zu 100% darauf!

Kläre am besten folgende Fragen, bevor du dich in einem sozialen Netzwerk im Internet engagierst:

**Was möchtest du mit deinem Profil erreichen?**
- Kontakte zu Freunden halten
- verlorene Kontakte wieder herstellen
- neue Kontakte knüpfen
- Arbeitgeber auf dich aufmerksam machen
- berufliche Kontakte knüpfen

**Wozu möchtest du dein Profil verwenden?**
- Selbstdarstellung
- Flirtprofil
- Bewerbungsprofil

**Ist die Angabe deines richtigen Namens unbedingt nötig?**

# Warum solltest du mit deinen Daten vorsichtig sein?

Auch wenn es einfacher ist, dich unter deinem echten Namen zu finden, solltest du die Risiken bedenken, die dadurch entstehen können, dass die „community“ diese Information hat.

Welche Risiken sich dadurch ergeben können, belegen folgende Beispiele aus der Presse:

- Bewerber wurden wegen Einträgen oder Fotos in sozialen Netzen, die nicht zur Einstellung der Firma passen oder auf mangelnde Arbeitsmoral schließen lassen, abgelehnt.
- Arbeitnehmern wurde wegen negativer Aussagen über ihren Arbeitgeber gekündigt.
- Politisch inkorrekte Aussagen führten zum Parteiausschluss bzw. Mandatsverlust.
- Schülerinnen und Schüler wurden wegen beleidigenden Äußerungen über ihren Lehrer von der Schule verwiesen.
- Daten aus sozialen Netzwerken wurden dafür genutzt, um Phishing-Mails bzw. E-Mail-Viren als echte Nachrichten von Freunden erscheinen zu lassen.

Phishing-Mails locken mit trickreichen Begründungen auf eine Webseite, die genauso aussieht wie die Startseite deiner Bank, deines E-Mail-Anbieters oder deines sozialen Netzwerks und versuchen so vertrauliche Daten von dir zu bekommen. Wenn der Absender solcher Mails Infos über dich hat (wie z.B. Wohnort, Musikvorlieben) oder sogar unter dem Namen eines Freundes schreibt, fällt die Täuschung viel leichter.

# Wer könnte künftig auch Interesse an deinen Daten haben?

- Versicherungen, die z.B. spezielle Risiken vor Abschluss von Lebens-, Berufsunfähigkeits-, Kranken- oder KFZ-Versicherungen ermitteln wollen.
- Auskunfteien, die Kreditwürdigkeit, Kaufkraft und das umsatzrelevante Verhalten (Viel- / Wenigtelefonierer) ermitteln wollen.
- Vermieter, die das Verhalten von Wohnungsbewerbern (häufige Partys, laute Musik, Haustiere, sonstige unerwünschte Vorlieben) ermitteln wollen.
- Arbeitgeber, die sich ein umfassenderes Bild über den Arbeitnehmer machen wollen oder nachweisen wollen, dass die Arbeitszeit privat genutzt wurde.

  oder

- Polizei und Geheimdienste, die Bilddaten nutzen könnten, um Personen auf Überwachungsvideos zu identifizieren. Vielleicht gibt es auch bald eine App, die die Profile fotografierter Personen ermittelt.

# 1. Du nutzt soziale Netzwerke privat: Verwende einen Spitznamen (Pseudonym)!

Einige soziale Netzwerke bieten ihren Nutzerinnen und Nutzern ausdrücklich an, öffentlich unter einem Spitznamen aufzutreten. Nutze diese datenschutzfreundliche Möglichkeit, um deine Identität nicht preisgeben zu müssen. Aber auch wenn es der Netzwerk-Anbieter nicht vorsieht: Bestimmungen in den „Allgemeinen Geschäftsbedingungen“, die eine Verwendung von Spitznamen verbieten, sind unwirksam, da die Betreiber nach § 13 Absatz 6 Telemediengesetz (TMG) verpflichtet sind, eine Nutzung ihrer Dienste unter Pseudonym zu ermöglichen.

# 2. Du willst im sozialen Netzwerk gefunden werden: Leg’ dafür ein zusätzliches Profil an!

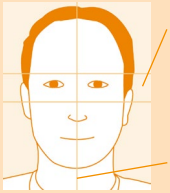
Ist es ausnahmsweise notwendig, dass du unter deinem echten Namen gefunden wirst, solltest du dafür ein zusätzliches Profil anlegen, das nur die zum Auffinden unbedingt notwendigen Daten (z.B. Stadt oder Hochschule) enthält. Zwar kann man in vielen Netzwerken die Sichtbarkeit von Profilinhalten beschränken, doch leider sind diese Funktionen oft nicht fehlerfrei.

Gib’ deinen „echten“ Namen nur bei der Anmeldung deines Profils an, falls das notwendig ist und denk’ daran, dass der Betreiber des Netzwerks Zugriff auf alle Daten deines Profils hat. Schau’ dir also an, wem du deine Daten anvertraust.

# 3. Du möchtest deine privaten Fotos veröffentlichen: Stell' keine Fotos ins Netz, auf denen du oder andere Personen erkennbar sind!

Überlege dir genau, ob die Fotos wirklich für die Öffentlichkeit oder ob sie z.B. nur für deine Freunde bestimmt sein sollen. Kann dir die Veröffentlichung vielleicht schaden? Schalte auf jeden Fall Funktionen aus, die dich automatisch auf Fotos erkennen. Sonst könntest du leicht auf anderen Fotos im Netz oder gar auf Überwachungsvideos – mit deiner Zustimmung – identifiziert werden. Idealerweise sollten Fotos nur dann in das Netzwerk eingestellt werden, wenn du oder andere Personen darauf nur von Freunden erkannt werden können.

Biometrische Fotos ermöglichen es Computern, dich besonders gut und schnell auf anderen, verschiedenen Fotos auf Grund deiner unverwechselbaren Merkmale (Augenabstand, Nasengröße etc.) wieder zu erkennen.




# 4. Du legst dein Profil im sozialen Netzwerk an: Veröffentliche nur die Daten, die notwendig sind, und nicht mehr!

Du solltest unbedingt den konkreten Zweck bestimmen, den dein Profil erfüllen soll und dir dann genau überlegen, welche Daten du über deine Person veröffentlichen willst.

Du hast im Alltag auch verschiedene Rollen (auf der Arbeit, privat bzw. bei Freunden, in der Familie, etc.) und entscheidest, wem du welche Information gibst. In sozialen Netzwerken kann man das noch nicht unterscheiden. Du kannst zwar Gruppen wie z.B. „Freunde" bilden, aber innerhalb der Gruppe bekommen auch alle die gleichen Informationen.

Daher solltest du für die unterschiedlichen sozialen Rollen auch verschiedene Profile mit den jeweilig passenden Daten anlegen.

Überlege dir, welche Sensordaten Smartphone Apps sozialer Netzwerke erhalten oder gar veröffentlichen dürfen.

Sensordaten: Smartphones und Wearables (z. B. smarte Uhren, Armbänder, Brillen) sind mit einer Menge von Sensoren ausgestattet, die Fitnesswerte und Gesundheitswerte (zurückgelegte Schritte, Puls, Hautwiderstand) sowie deinen Aufenthaltsort und damit deinen Tagesablauf ermitteln können. Bedenke, dass z. B. Hautwiderstand und Puls Messwerte bei Lügendetektoren sind.

# 5. Behalte die Kontrolle: Gib' deine Kontaktdaten nicht an!

Die Angabe von Kontaktdaten (z.B. Telefonnummer, Postadresse) ist nicht notwendig, da jedes Netzwerk interne Kontaktmöglichkeiten bereitstellt. Sicher ist es praktisch, soziale Netzwerke als Adressbuch zu nutzen, allerdings sind die Kontaktdaten dann öffentlich zugänglich – zumindest für alle Online-Freunde, von denen sicher nicht alle echte Freunde sind. Zudem werden die Daten auf Servern im Internet gespeichert, die für Hacker wegen der großen Datenmengen sehr lukrativ sind. Manche Netzwerke nutzen die Kontaktdaten auch für die Zusendung von Werbung. Dies ist für Telefon-, Fax- und E-Mail-Werbung nur erlaubt, wenn es dem Betreiber (freiwillig!) ausdrücklich gestattet wurde.

Hacker nutzen Lücken oder Fehler in Programmen, um über Netzwerke auf Daten zuzugreifen, die eigentlich nicht für sie zugänglich sein sollten – wie z.B. deine Passwörter.

# 6. Leg' fest, wer dein Profil sehen kann: Beschränke den Datenzugriff!

Bei den meisten Netzwerken kannst du festlegen, welche Daten öffentlich, d.h. für alle Nutzer des Netzwerks oder sogar für alle Internetnutzer oder nur für Freunde zugänglich sein sollen. Diese Einstellmöglichkeit findest du meist unter „Privacy / Privatsphäre" oder „Mein Profil". Du solltest immer die restriktivsten Einstellungen wählen. Besonders wichtig ist, dass deine „Freundesliste" nicht öffentlich ist, da sich sonst auch über deine Freunde viele Informationen zu dir besorgt werden können. Du solltest es auch nicht ermöglichen, dass Fotos oder Videos von Anderen unkontrolliert mit deinem Profil verlinkt oder Nachrichten an dich in ein öffentlich lesbares Forum oder Gästebuch geschrieben werden können. In einem Profil sollten wirklich nur die Informationen öffentlich gemacht werden, die jedem beliebigen Fremden unbedenklich mitgeteilt werden können.

„Restriktiv" bedeutet eingeschränkt. Deine Interessen, dein Geburtsdatum, deine Fotoalben und auch dein richtiger Name sollten höchstens für echte Freunde zugänglich sein. Es muss auch nicht jedes Feld im Profil ausgefüllt sein: Daten, die nicht zugänglich sind, können nicht missbraucht werden.

# 7. Leg' fest, wer dein Profil im Netzwerk finden kann: Beschränke den Datenzugriff auf Mitglieder und schließe ihn für Suchmaschinen aus!

In einigen Netzwerken können Profildaten grundsätzlich nur von anderen Mitgliedern gelesen werden, andere bieten den Ausschluss von Suchmaschinen oder die Beschränkung des Zugriffs auf Mitglieder zumindest als Option. Wird diese Option nicht gewählt, so findet sich das Profil später nicht nur bei Google, sondern auch in den Ergebnislisten spezialisierter Personensuchmaschinen wie yasni.de wieder. Daher solltest du Internet-Suchmaschinen grundsätzlich ausschließen.

Die großen Suchmaschinen bieten an, veraltete Suchergebnisse – also z. B. gelöschte, geänderte oder für Suchmaschinen gesperrte Einträge in den Ergebnislisten zu aktualisieren bzw. zu entfernen. Schau dir dazu die Hilfeseiten der Suchmaschinen an.

Im Mai 2014 hat zudem der Europäische Gerichtshof entschieden, dass Suchmaschinen auch Links zu existierenden Webseiten entfernen müssen, wenn diese die Persönlichkeitsrechte verletzten und das Informationsrecht der Öffentlichkeit nicht überwiegt. Auch dazu finden sich Hinweise bei den Suchmaschinenbetreibern. Allerdings sollte man immer zuerst versuchen, die Daten auf der Original-Webseite zu entfernen.

# 8. Was brauchst du wirklich: Ermögliche Anwendungen von Dritten keinen Zugriff auf deine Profildaten!

Einige Netzwerkbetreiber ermöglichen Anderen, Anwendungen mit mehr oder weniger nützlichen oder lustigen Zusatzfunktionen (z.B. Verschicken von Herzen an Freunde oder die Anzeige des aktuellen Wetterberichts) zu programmieren. Dazu muss oftmals auf deine Profildaten zurückgegriffen werden. Dabei ist es möglich, dass diese Anwendungen weitere (nicht erwünschte) Zwecke, ähnlich einer Spy- oder Adware, verfolgen. Das könnte z.B. das Auskundschaften deiner Nutzerdaten für zielgerichtete Werbung sein. Du solltest dir genau überlegen, ob und in welchem Umfang du Zugriffsrechte auf deine Profildaten einräumst.

Spyware nennt man Schnüffelprogramme, die neben ihrer offiziellen Aufgabe noch andere Funktionen haben, z.B. Dateien auf deinem Computer auszuspionieren und ohne dein Wissen weiterzugeben oder auch dein Verhalten im Netz nachzuvollziehen.

# 9. Du willst deine Daten schützen: Vorsicht bei netzwerkübergreifenden Verknüpfungen!

Soziale Netzwerke oder zusätzliche Dienstleister bieten dir manchmal die Möglichkeit, dass Profildaten in mehreren Netzwerken gemeinsam gepflegt bzw. in anderen Zusammenhängen – z.B. auf kooperierenden Webseiten genutzt werden. Stell' dein Profil lieber so ein, dass die Datennutzung außerhalb der eigentlichen Plattform grundsätzlich verhindert wird. Die Login-Daten sollten immer nur auf der Plattform selbst eingegeben werden. Willst du eine solche Verknüpfung dennoch nutzen, so solltest du dich genau informieren, wer Zugriff auf welche deiner Dateien erhält. Sei besonders vorsichtig bei Diensten, die eine Art „Startseite" zu allen Profilen in sozialen Netzwerken anbieten, da hier die Login-Daten aller Profile mit übergeben werden. Datendiebe hätten so mit einem Schlag Zugriff auf alle deine Accounts.

Mit Facebook „Connect" brauchst du z.B. auf einer Spielewebseite keinen neuen Account anlegen, sondern spielst unter deinem Facebook-Namen und kannst einfach deine Freunde einladen und gegen sie spielen. Das Problem ist nun, dass die Spielewebseite sowohl auf deine Profildaten, als auch auf die deiner Freunde zugreifen kann.

# 10. Du willst keinen Ärger mit Anderen: Beachte die Rechte Dritter!

Ein leichtfertig veröffentlichtes Foto oder ein Kommentar in einem Gästebuch können dich und andere schnell in eine unangenehme Situation bringen.

Du solltest daher stets um Erlaubnis bitten, bevor du ein Foto, Video oder auch Text von oder über jemand anderen veröffentlichst. Dies gilt insbesondere, wenn das Material mit Informationen zu denjenigen (z.B. mit Fotos) verlinkt wird.

# Warum interessiert sich die Wirtschaft für deine Daten?

Soziale Netzwerke erfassen erstmals die Verbindungen ihrer Nutzerinnen und Nutzer, ihre Bekanntschafts- und Freundschaftsbeziehungen untereinander.

Daraus können Datenbanken erstellt werden, die als „Social Graph“ bezeichnet werden.

Die wirtschaftliche Auswertung dieser Datenbanken entwickelt sich gerade zu einem spannenden neuen Geschäftsfeld.

Es gibt z.B. bei Facebook die Funktion „Beacon“, die deinen Freunden automatisch anzeigt, welche Filme oder Bücher du online gekauft oder ausgeliehen hast, um durch deine „Empfehlung“ möglichst weitere Bestellungen zu erzielen. Um das zu verhindern, muss diese Funktion extra ausgeschaltet werden.

## Fazit

**Soziale Netzwerke sind eine tolle Kommunikationsform und wenn du unsere 10 Tipps beachtest, schützt du mit einfachen Mitteln deine Privatsphäre ohne auf die Vorteile zu verzichten.**

# Hier findest du mehr Informationen:

**www.datenschutz.de**
Gemeinsames Portal der Datenschutzinstitutionen der Länder und des Bundes sowie der Kirchen in Deutschland und einiger Institutionen aus dem Ausland. Hier findest du unter anderem Informationen dazu, welche Ansprechpartner du in welchen Fällen von Datenmissbrauch kontaktieren musst.

**www.datenschutz-berlin.de**
Die Website des Berliner Beauftragten für Datenschutz und Informationsfreiheit.

**www.bfdi.bund.de**
Die Website des Bundesbeauftragten für Datenschutz und Informationsfreiheit.

**www.bfdi.bund.de/bfdi_forum**
Das Datenschutzforum. Hier kannst du Fragen rund um das Thema Datenschutz stellen, die von anderen Forumsmitgliedern mit viel Fachwissen beantwortet werden. Außerdem führt der Bundesdatenschutzbeauftragte hier seinen Blog.

**www.watchyourweb.de**
Eine Initiative von „Jugend online“. Hier findest du Antworten zu allen Fragen, die deine Daten im Netz betreffen. In einem Test findest du heraus, welcher Web-Typ du bist und regelmäßige Aktionen wie Foto- und Videowettbewerbe sorgen dafür, dass Datenschutz hier auch noch Spaß macht.

**www.netzcheckers.de**
Das Jugendportal für digitale Kultur bietet neben Anleitungen zur Einstellung der Privatsphäre in Social Networks unter dem Stichwort „Deine Sicherheit in Sozialen Netzwerken“ jede Menge weiteres Medien-Know-How.

**www.klicksafe.de**
Die EU-Initiative für mehr Sicherheit im Netz. In der Rubrik „Communities & Social Networks“ erklärt klicksafe die Unterschiede zwischen Foren, sozialen Netzwerken und Web-2.0-Portalen wie Youtube. Flyer für Eltern und Unterrichtsmaterial für Lehrkräfte können als PDF heruntergeladen oder bestellt werden.

**www.irights.info**
Die Initiative iRights.info informiert seit Jahren aus juristischer Sicht und in einfacher Sprache über Urheberrechte in der digitalen Welt. In Kooperation mit klicksafe entstand ein lesenswerter leicht verständlicher Grundlagenartikel zu „Urheber- und Persönlichkeitsrechten in sozialen Netzwerken“.

**www.youngdata.de**
Eine Informationsseite des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz zu Selbstschutz bei aktuellen Internetdiensten, insbesondere für Jugendliche.

**www.jugendnetz-berlin.de**
Hier findest du neben vielen medienpädagogischen Angeboten auch aktuelle Nachrichten zu den Themen Datenschutz, Medienkompetenz und vieles mehr.

**selbst & bewusst**
Tipps für den persönlichen Datenschutz bei Facebook. Eine Broschüre des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, zu finden unter www.datenschutz.hamburg.de

# Impressum

**Herausgeber:**

**Berliner Beauftragter für Datenschutz und Informationsfreiheit**
**Anschrift:**
Friedrichstr. 219
10969 Berlin

**Sprechzeiten:**
Mo.- Fr., 10.00 – 15.00 Uhr
Do., 10.00 – 18.00 Uhr
Besuchereingang:
Puttkamer Str. 16-18

**Kontakt:**
Telefon: 030/13 88 90
Telefax: 030/21 55 05 0
mailbox@datenschutz-berlin.de

**Landesprogramm jugendnetz-berlin**

**Anschrift:**
Jugend- und Familienstiftung
des Landes Berlin - Projektbüro
Obentrautstr. 55
10963 Berlin

**Kontakt:**
Telefon: 030/70728531
go@jugendnetz-berlin.de

**Redaktion:**
Oliver Berthold
Referent beim
Berliner Beauftragten
für Datenschutz und
Informationsfreiheit

Astrid Dinges
Uta Voigt
Sabine Quandt
music media park e.V.

**Gestaltung:**
Gabriel Braun

**Druck:**
Pinguin Druck GmbH, Berlin

**11. Auflage**
**Gesamtauflage:** 35.000
**Stand:** Dezember 2014, Berlin

Jeder kann sich an den Berliner Beauftragten für Datenschutz und Informationsfreiheit wenden, wenn er der Ansicht ist, dass bei der Verarbeitung personenbezogener Daten gegen Datenschutzvorschriften verstoßen wurde.

Ziel des Berliner Landesprogramms jugendnetz-berlin ist die Förderung von Kindern und Jugendlichen für einen selbstbestimmten, kreativen und verantwortungsvollen Umgang mit Medien, als Voraussetzung für Teilhabe und Beteiligung in der digitalen Gesellschaft.

In allen 12 Berliner Bezirken entwickeln, vernetzen und unterstützen Medienkompetenzzentren eine Vielzahl von medienpädagogischen Angeboten und Modellprojekten. Kooperationspartner sind u.a. die Initiative comp@ss – Computerführerschein, Bits 21 - Fortbildung von Fachkräften und das Netzwerk der Berliner Jugendkulturzentren.
Neu ist der Aktionsfonds JuMP (Jugend- und Medienprojekt) bei dem junge Menschen über die Mittel zur Umsetzung eigener Medienprojekte selbst entscheiden können. Ende 2015 wird das Jugendportal BERLIN an den Start gehen, welches neben vielen Informationen für Jugendliche und einem von Jugendlichen gestalteten crossmedialen Medienmagazin auch Möglichkeiten zur digitalen Beteiligung bieten wird.

Das Berliner Landesprogramm jugendnetz-berlin wird von der Senatsverwaltung für Bildung, Jugend und Wissenschaft und der Jugend- und Familienstiftung des Landes Berlin gefördert und gemeinsam in Kooperation mit den Berliner Bezirken umgesetzt.

jugendnetz-berlin.de

Berliner Beauftragter für
Datenschutz und Informationsfreiheit

jfsb
Jugend- und Familienstiftung
des Landes Berlin
Stiftung des öffentlichen Rechts

be Berlin
Senatsverwaltung
für Bildung, Jugend
und Wissenschaft