

## → Bitte beachten

Jede Internetseite muss eine Datenschutzerklärung enthalten. Dies muss eine extra Seite sein, die von jeder anderen Unterseite aus erreichbar ist. In der Datenschutzerklärung muss über die Verarbeitung der personenbezogenen Daten der Nutzer\*innen informiert werden. Auch IP-Adressen gelten als personenbezogene Daten.

## Vertrauenswürdige Selbsthilfeforen finden

Kennen Sie die GRÜNEN ADRESSEN der NAKOS? Dort finden Sie auch Selbsthilfe-Internetforen, bei denen der Schutz personenbezogener Daten besonders ernst genommen wird.

[www.nakos.de/adressen/gruen/selbsthilfe-internetforen](http://www.nakos.de/adressen/gruen/selbsthilfe-internetforen)

## Weitere Informationen

- Rubriken **Selbsthilfe im Internet** und **Datenschutz** auf [nakos.de](http://nakos.de)
- Beispielhomepage für die Selbsthilfe auf [nakos.de](http://nakos.de)
- **Umsetzungshilfe zur DSGVO**  
Herausgeber: NAKOS, 2019

## Digitale Anwendungen bieten der Selbsthilfe vielfältige Chancen:

Selbsthilfegruppen nutzen digitale Anwendungen im Internet, um auf sich aufmerksam zu machen. Menschen mit gleicher Betroffenheit können zueinander finden und sich austauschen, auch über große Distanzen hinweg. Vieles was in der Selbsthilfe besprochen wird, ist jedoch sehr persönlich. Es geht um Erkrankungen, schwierige Lebenssituationen, zum Teil auch um tabuisierte Themen. Da das Internet ein öffentlicher Raum ist, ist es erforderlich, persönliche Informationen der Beteiligten so gut wie möglich zu schützen. Dies wird auch von der im Mai 2018 in Kraft getretenen europäischen Datenschutzgrundverordnung (DSGVO) so verlangt. Dieses Faltblatt enthält wichtige Hinweise für diejenigen, die für ihre Selbsthilfefragen ins Internet gehen und digitale Anwendungen nutzen. Sei es, dass sie Anwendungen von Anderen nutzen oder eigene Informations- oder Austauschangebote zur Verfügung stellen.



# NAKOS

Nationale Kontakt- und Informationsstelle zur Anregung und Unterstützung von Selbsthilfegruppen

Otto Suhr-Allee 115, 10585 Berlin  
Telefon: 030 | 31 01 89 -60  
Fax: 030 | 31 01 89 -70  
E-Mail: [selbsthilfe@nakos.de](mailto:selbsthilfe@nakos.de)

Das Wissensportal zur Selbsthilfe:  
[www.nakos.de](http://www.nakos.de)

Eine Einrichtung der  
Deutschen  
Arbeitsgemeinschaft  
Selbsthilfegruppen e.V.



Gefördert von:  
Bundesministerium  
für Gesundheit



aufgrund eines Beschlusses  
des Deutschen Bundestages

# DIGITALE SELBSTHILFE

## So schütze ich meine Daten und die Daten von anderen

## TRACKING

### Tracking – beim Surfen über die Schulter geschaut

Beim Tracking wird das Surfverhalten von Personen erfasst und zu Nutzerprofilen zusammengeführt. Dies geschieht zumeist mit dem Ziel, personalisierte Werbung einblenden zu können. Beim Besuch einer Internetseite ist zumeist nicht erkennbar, ob getrackt wird oder nicht. Die Nutzer\*innen sehen nicht, an wen ihre Daten fließen und es gibt zumeist auch nicht die Möglichkeit, dem zu widersprechen.

### Hier kommt es zum Tracking

- bei „Social-Plug-Ins“ (z.B. Facebook, Google+, YouTube)
- bei Werbeanzeigen (z.B. von Google, Amazon)
- bei vielen kostenfreien E-Mail-Anbietern (z.B. Gmail), Hosting und Cloud-Diensten
- (vermutlich) bei kostenfreien Angeboten von Google wie Google Maps, Google Kalender, Google Suchfunktionen, Google Schriften

# DIGITALE ANWENDUNGEN NUTZEN

## → Bitte beachten

Gehen Sie sorgsam mit Angaben zu Ihrer Person, zu Ihrer Erkrankung und zu Ihren Lebensumständen um. Denken Sie daran, dass Ihre privaten Angaben unter Umständen auch von Dritten gelesen werden. Vermeiden Sie zudem Angebote, bei denen Ihr Surfverhalten erfasst und analysiert wird (Tracking).

## E-MAILS ✓

- Nutzen Sie keine E-Mail-Dienstleister, die die Inhalte von E-Mails auslesen. Dies ist bei vielen kostenfreien Angeboten wie z. B. Google der Fall.
- Überlegen Sie, eine E-Mail-Adresse zu wählen, die keinen Bezug zu Ihrem Namen zulässt (z. B. km@online.de anstelle klaus.mustermann@online.de).
- Nutzen Sie verschiedene E-Mail-Adressen, je nachdem ob Sie sich privat austauschen, in Foren registrieren, Bestellungen im Internet tätigen oder beruflich kommunizieren.
- Informieren Sie sich über Möglichkeiten, E-Mails zu verschlüsseln.

## MESSENGER DIENSTE ✓

- WhatsApp empfiehlt sich nicht für die Kommunikation über sensible Themen. Für die Kommunikation einer Selbsthilfegruppe sollten sichere, nicht-trackende Alternativen wie Wire, Threema oder Telegram gewählt werden.

## PASSWÖRTER ✓

- Achten Sie auf sichere Passwörter und ändern Sie diese regelmäßig. Tipp: Nutzen Sie dafür einen Passwortmanager (z. B. lastpass.com/de).

## SUCHMASCHINEN ✓

- Nutzen Sie Suchmaschinen, bei denen Ihr Suchverhalten nicht verfolgt wird (z. B. startpage.de, duckduckgo.com).

## SOZIALE NETZWERKE ✓

- Vermeiden Sie den Austausch über Erkrankungen oder schwierige Lebensumstände in Sozialen Netzwerken (z. B. Facebook). Nutzen Sie dafür lieber Angebote, bei denen Ihr Suchverhalten nicht verfolgt wird.
- Achten Sie darauf, Ihre Profile in Sozialen Netzwerken vor den Blicken „Unbefugter“ zu schützen.
- Überprüfen Sie die entsprechenden Einstellungen regelmäßig, da die Betreiber immer wieder Änderungen vornehmen, die Auswirkungen auf Ihre Einstellungen haben können.

## SICHERE VERBINDUNGEN ✓

- Mit der Browsererweiterung HTTPS-Everywhere können Sie sicherstellen, dass die Datenübertragungen zwischen Ihnen und Internetseiten verschlüsselt ablaufen.
- Nutzen Sie Browsererweiterungen (z. B. Flagfox), um zu erfahren, wo der Server einer Internetseite steht.

## TRACKING ERKENNEN UND ERSCHWEREN ✓

- Nutzen Sie Browsererweiterungen, die Ihnen zeigen, ob Sie beim Besuch von Internetseiten getrackt werden (z. B. Ghostery, Lightbeam, HTTP-Fox).
- Nehmen Sie Einstellungen in Ihrem Browser vor, die Tracking erschweren. Lassen Sie z. B. bei jedem Schließen des Browsers die Cookies löschen (z. B. über die Browsererweiterung BetterPrivacy).
- Nutzen Sie verschiedene Browser: z. B. einen für privates Surfen und einen anderen für das Surfen in Sozialen Netzwerken. Oder Sie surfen anonym über das Anonymisierungsnetzwerk TOR.

# DIGITALE ANWENDUNGEN ZUR VERFÜGUNG STELLEN

## → Bitte beachten

Für alle Angebote zur gemeinschaftlichen Selbsthilfe, bei denen digitale Anwendungen genutzt werden gilt: Erheben und veröffentlichen Sie so wenig personenbezogene Daten wie möglich. Das deutsche Datenschutzrecht mahnt zur Datensparsamkeit. Angebote im Internet sollen nicht mehr personenbezogene Daten erheben, als unbedingt notwendig ist. Angaben zur gesundheitlichen Situation etwa zu Beschwerden, Diagnosen oder Behandlung gelten in Verbindung mit personenbezogenen Informationen wie Name, Alter oder Geschlecht als besonders schützenswert.

## TECHNISCHE VORAUSSETZUNGEN SCHAFFEN ✓

- Erstellen Sie Ihr Angebot nicht mit Webseitenbaukastensystemen und bei externen Hostinganbietern, die dies mit dem Tracking (Nachverfolgen) der Nutzer\*innen Ihres Angebots verbinden.
- Hosten Sie Ihr Angebot auf dem Server eines seriösen Anbieters aus Deutschland. Dieser unterliegt der deutschen Datenschutzgesetzgebung.
- Führen Sie regelmäßige Updates für die Software durch, mit der Ihr Angebot programmiert ist.
- Achten Sie darauf, dass Datenübertragungen zwischen den Nutzer\*innen und Ihrem Internetangebot verschlüsselt erfolgen.
- Informieren Sie die Nutzer\*innen Ihres Angebots darüber, was Sie mit den erhobenen Daten machen (Datenschutzerklärung).
- Überlegen Sie, ob die Beiträge in Ihrem Forum von Suchmaschinen durchsucht werden sollen und verhindern Sie dies gegebenenfalls.

## DATENSPARSAMKEIT BEACHTEN ✓

- Veröffentlichen Sie so wenig personenbezogene Angaben wie möglich auf Ihrem Internetangebot (z. B. bei den Angaben zu Kontaktpersonen von Selbsthilfegruppen).
- Wenn sich Nutzer\*innen auf Ihrem Internetangebot registrieren können, beschränken Sie sich auf die Abfrage eines selbst wählbaren Nutzernamens und einer E-Mail-Adresse. Verzichten Sie auf die Abfrage von Klarnamen, Adresse, Telefonnummer, Angaben zur Erkrankung / zum Problem.

## PERSONENBEZOGENE ANGABEN SCHÜTZEN ✓

- Meiden Sie Anwendungen, die das Verhalten der Nutzer\*innen auf Ihrer Internetseite auswerten, verfolgen und analysieren (Tracking). Vorsicht insbesondere bei kostenfreien Angeboten kommerzieller Anbieter (z. B. Schriften, Landkarten, Suchfunktionen oder Analyseprogramme, Clouds).
- Wenn Sie das Verhalten der Nutzer\*innen auf Ihrer Internetseite auswerten wollen, nutzen Sie Analyseprogramme, die nicht tracken (z. B. Matomo).
- Binden Sie keine „Social Plug-Ins“ ein wie den „Gefällt mir“-Button von Facebook. Diese tracken die Nutzer\*innen Ihrer Internetseite. Verwenden Sie stattdessen „2 Klick-Lösungen“, bei denen die Nutzer\*innen selbst entscheiden können, ob sie einer Datenübertragung zustimmen.
- Wenn Sie eine E-Mail an mehrere Empfänger versenden, setzen Sie die Adressen in „Blind Copy“, damit diese nicht für alle Empfänger sichtbar sind (bcc statt cc).
- Schicken Sie sensible Daten besser nicht per (unverschlüsselter) E-Mail.

## SOZIALE NETZWERKE ✓

- Nutzen Sie Soziale Netzwerke möglichst nur für die Öffentlichkeitsarbeit, zum Beispiel um Ihre Selbsthilfegruppe oder Selbsthilfevereinigung bekannt zu machen. Bieten Sie Austauschangebote besser auf Ihrer eigenen Internetseite an.