Der Landesbeauftragte
für den Datenschutz Rheinland-Pfalz

Orientierungshilfe

Selbst-Datenschutz in sozialen Netzwerken

Hintere Bleiche 34 | 55116 Mainz
Postfach 30 40 | 55020 Mainz
Telefon +49 (0) 6131 208-2449
Telefax +49 (0) 6131 208-2497
poststelle@datenschutz.rlp.de
www.datenschutz.rlp.de

Es gibt nix Gutes, außer man tut es – SELBST!

Tipps und Tricks zum Selbst-Datenschutz in sozialen Netzwerken

Bei den sozialen Netzwerken handelt es sich um Internetplattformen, auf denen man sich selbst darstellen, mit anderen vernetzen und sich mit Ihnen online treffen kann. Hierzu stellen die Mitglieder dieser virtuellen Gemeinschaften Profile über sich ins Netz. Diese Profile bestehen aus persönlichen Angaben, etwa dem Namen, dem Alter, den persönlichen Interessen und ggf. auch der privaten Postanschrift. 60 % aller Netzwerker zeigen sich auf Fotos, 40 % gemeinsam mit ihren Freunden oder Familienmitgliedern.

Mit Hilfe dieser Profile können Kontakte geknüpft, alte Freunde wieder gefunden, Gleichgesinnte aufgespürt oder Freundschaften gepflegt werden. So entsteht ein auf Kommunikation gestütztes Beziehungsgeflecht, ein soziales Netzwerk („social community“). Aktuellen Studien zufolge sind rund 85 % der Deutschen Mitglied in einem solchem Netzwerk. Die bekanntesten sind schülerVZ, studiVZ, facebook, mySpace, wer-kennt-wen, die lokalisten und XING.

Diese Netzwerke haben auch ihre Schattenseiten. Da grundsätzlich jeder Mitglied werden kann und auch die Betreiber der Netzwerke ihre kommerziellen Interessen verfolgen, muss sich der Nutzer darüber im Klaren sein, dass seine eingestellten Daten auch für ganz andere Zwecke genutzt werden können, z.B. für (personalisierte) Werbung oder für Recherchen von Arbeitgebern, Auskunfteien, Versicherungen, Journalisten oder Sicherheitsbehörden.

Ein besonderes Problem stellt das Cybermobbing dar. Stalker und Mobber missbrauchen Daten, die sie in den Netzwerken finden, um ihre Opfer zu diffamieren oder Lügen über sie zu verbreiten.

Dieser Flyer soll Ihnen mit Tipps und Tricks helfen, die Vorteile der Netzwerke zu nutzen, mitzumachen ohne zu bereuen.

Tipps zum Selbst-Datenschutz in sozialen Netzwerken

1. Ganz genau hinschauen!

Das Angebot im Internet ist unüberschaubar vielfältig. Bedenken Sie, dass es unterschiedliche Netzwerke für verschiedene Zwecke gibt und überlegen Sie genau, an welcher Stelle Sie welche persönliche Information preisgeben. Im Internet sollte man grundsätzlich nur die Daten von sich preisgeben, die man auch einem Fremden mitteilen würde. Prüfen Sie sorgfältig, welche Daten für das von Ihnen genutzte Netzwerk erforderlich sind.

2. AGB lesen!

Bei den Anbietern sozialer Netzwerke handelt es sich nicht um gemeinnützige Einrichtungen, sondern um gewinnorientierte Unternehmen. Die Netzwerke finanzieren sich weitgehend durch Werbung. Zum Teil werden Daten an die Werbewirtschaft weitergegeben, zum Teil werden die Daten für die Werbewirtschaft genutzt. Ziel jeder wirtschaftlichen Verwertung ist dabei die sog. personalisierte Werbung, d.h. jene Werbung, die mit Hilfe der Netzwerkangaben auf den jeweiligen Nutzer zugeschnitten ist. Den eigentlichen Wert des Unternehmens bilden daher die von den Nutzern eingestellten Daten. Lesen Sie in den Allgemeinen Geschäftsbedingungen (AGB) nach, was der Anbieter mit Ihren Daten vorhat, insbesondere wenn Sie die Community verlassen und Ihre Daten löschen möchten.

3. Flunkern erlaubt!

Wenn Sie mithilfe eines Netzwerks neue Freundschaften schließen möchten, ist es nicht erforderlich, dort mit dem richtigen Namen aufzutreten. Benutzen Sie daher in solchen Netzwerken ein Pseudonym (Spitzname). Die Nennung des richtigen Namens ist nur in solchen Netzwerken sinnvoll, in denen man alte Freunde wieder finden möchte. Aber auch dann sollte man sich überlegen, zumindest den Nachnamen über die Privatsphäreeinstellungen zum Initial abzukürzen.

4. Ändern Sie die Standardeinstellungen!

Wenn Sie sich angemeldet und nichts an den vorgegebenen Einstellungen geändert haben, kann es passieren, dass Ihr Name und Profil über Suchmaschinen weltweit recherchierbar ist. Denn die meisten Anbieter sozialer Netzwerke haben die Privatsphäre-Einstellungen auf unsicherster Stufe voreingestellt. Nutzen Sie die vorhandenen Einstellungsmöglichkeiten und

machen Sie Ihre Daten - am besten sofort nach der Anmeldung - nur bestimmten Nutzern zugänglich.

5. Das Netz vergisst nichts! Weniger ist daher mehr!

Beachten Sie auch, dass grundsätzlich jeder Mitglied der Community werden kann und Sie die Identität eines anderen nicht überprüfen können. Selbst wenn der Profilsteckbrief mit vielen Feldern lockt: Kategorien können auch offen bleiben. Geben Sie daher niemals Ihre Postanschrift oder Telefonnummer an. Stellen Sie auch keine heiklen Inhalte ins Netz. Informationen über politische Einstellungen, sexuellen Vorlieben, religiöse Überzeugungen oder den Gesundheitszustand haben in öffentlichen Netzen nichts verloren.

Informationen, die einmal im Internet sind, kann man nicht einfach wieder löschen. Die Inhalte können zwischenzeitlich heruntergeladen, kopiert, verlinkt oder in Archivdatensätzen vorgehalten werden. Über den Zwischenspeicher („Cache“) von Suchmaschinen lassen sich auch vermeintlich gelöschte Einträge wieder sichtbar machen. Bedenken Sie, dass auch (künftige) Arbeitgeber, Versicherungen, Auskunfteien, Vermieter, Journalisten oder auch Sicherheitsbehörden Informationen über Sie einholen können.

6. Sie wissen nicht, wie sicher Ihre Daten sind!

Beachten Sie auch, dass die Netzwerkbetreiber ihre Systeme nicht immer sicher gegen Angriffe von außen abschirmen. Ein illegaler massenhafter Datenexport von Profilen ist bereits vorgekommen. Auch ist kaum eine Plattform dazu geeignet, in einem öffentlichen drahtlosen Netzwerk, etwa in Internetcafes, Bahnhöfen oder dergleichen, genutzt zu werden. Angreifer können leicht den Datenverkehr im Klartext mitlesen und sich in die laufende Nutzersitzung „einklinken“. Bei einigen Plattformen ist in WLAN-Netzen sogar das Nutzerkennwort gefährdet, da es unverschlüsselt übertragen wird. Wird dieses Kennwort auch für andere Dienste verwendet (z.B. für das E-Mail-Postfach), entsteht ein noch größeres Gefährdungspotenzial.

7. Achten Sie auf Ihren Umgang!

Bei manchen Netzwerken – etwa bei schülerVZ und wer-kennt-wen – gibt es sog. Gruppen. Ihre Zahl geht in die Hunderttausende. Zum Teil sind sie lustig („Gott erfand die Neugierde und nannte sie Mutter“) und informativ („Leben mit Diabetes“; „Koch- und Backrezepte“), zum Teil aber auch problematisch („Kiffen ist gesund“; „Wer tanzt, hat bloß kein Geld zum Saufen“).
Da es immer häufiger vorkommt, dass Personalchefs vor der Einstellung von Mitarbeitern im Internet recherchieren, sollte man sich problematische Gruppenmitgliedschaften ersparen. Die Gruppenzugehörigkeit kann mehr über

ein Mitglied aussagen als dessen Profil.

8. **Netzwerkübergreifendes Zusammenführen der Daten verhindern!**

   Die Profile, die Sie in den verschiedenen Netzwerken hinterlegt haben, können (z.B. über das „Googeln“ Ihrer E-Mail-Adresse) Ihrem Namen zugeordnet und damit zusammengeführt werden. Daher sollten für unterschiedliche soziale Rollen auch verschiedene Profile (Pseudonyme) und verschiedenen E-Mail-Adressen verwendet werden. Laden Sie deshalb auch kein (Pass-) Foto von sich hoch, aus dem einfach biometrische Merkmale extrahiert werden können; über Gesichtserkennungsdienste könnte man Ihre Daten zusammenführen.

9. **Rechte Dritter beachten!**

   Dritte können in sozialen Netzwerken leicht in unangenehme Situationen gebracht werden. Dazu gehört u.U. bereits ein leichtfertig veröffentlichtes Bild oder ein Kommentar in einem Gästebuch. Ohne Einwilligung des Betroffenen dürfen Fotos oder Videos nicht im Internet veröffentlicht werden. Dies kann sogar strafbar sein. Achten Sie die Privatsphäre anderer und beteiligen Sie sich nicht an Mobbing. Das Internet ist weder anonym noch ein rechtsfreier Raum. Nutzen Sie die Meldefunktionen der Anbieter, wenn Sie Verstöße gegen den Verhaltenskodex des Netzwerks oder gegen sonstige Regeln bzw. Gesetze feststellen.

10. **Überlassen Sie Kinder nicht sich selbst!**

    Jugendgefährdende Inhalte, Mobbing und „Abzocke“ machen auch vor Netz-Communities nicht halt. Kinder und Jugendliche sind häufig sehr viel freizügiger im Umgang mit ihren Daten und übernehmen weitaus häufiger ungeprüft die Standardeinstellungen der Betreiber. Kinder und Jugendliche bedürfen daher eines besonderen Schutzes, dem längst nicht alle Netzbetreiber Rechnung tragen. Informieren Sie sich bei Ihren Kindern über die derzeit „angesagten“ Communities und nehmen Sie am besten gemeinsam die Anmeldeprozedur vor. Beachten Sie: Für Kinder gibt es eigene Netzwerke, die die Eltern nicht außen vor lassen z.B. tivi-treff (http://www.tivi.de/tivi/tivitreff/start/index.html), freundebuch (http://www.das-freundebuch.de/), netztreff (http://www.kindernetz.de/netztreff), was ist was Klub (http://www.wasistwas.de/), wilden-hühner-community (http://community.wildehuehner.de/).

11. **Der Letzte macht das Licht aus!**

    Wer sein Netzwerk nicht mehr nutzen will, sollte seine Mitgliedschaft aufgeben und seine Profildaten löschen. Bei einigen Netzwerken ist dies mit wenigen Mouseklicks erledigt. Bei anderen Plattformen ist die Abmeldeprozedur aufwändig. Teilweise ist ein reguläres Löschen gar nicht vorgesehen, sondern nur

ein Deaktivieren der Daten. Der Aufwand lohnt sich aber. Sonst bleiben die eigenen Daten für immer im Netz. Im richtigen Leben macht man ja auch das Licht aus und die Tür zu, wenn man geht.

12. Informieren Sie sich und vertrauen Sie Ihrem gesunden Menschenverstand!

Das Internet ist eine tolle Erfindung und bietet riesige Möglichkeiten. Aber es ist wie im richtigen Leben: Man bekommt nichts umsonst, man kann nicht jedem trauen – kurz: Man muss sich vorsehen!

Prüfen Sie gelegentlich, was im Internet über Sie selbst zu finden ist. Hierzu gibt es spezielle Personensuchmaschinen, wie z.B. Spock.com, yasni.de oder 123people.de. Es gibt auch Dienstleister, die Ihnen diese Arbeit gegen Geld abnehmen und sich um Ihren guten Ruf im Internet kümmern.
Informieren Sei sich über Gefahren oder fragen Sie jemanden, der sich auskennt. Setzen Sie sich entweder mit dem Datenschutz- oder dem Jugendschutzbeauftragten Ihres Netzwerks in Verbindung oder wenden Sie sich an die zuständige staatliche Datenschutzaufsichtsbehörde. Dies sind – abhängig vom Sitz des Unternehmens – beispielsweise für

wer-kennt-wen:
Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen; poststelle@ldi.nrw.de

schülerVZ, studiVZ, meinVZ:
Der Berliner Beauftragte für Datenschutz und Informationsfreiheit; mailbox@datenschutz-berlin.de

die lokalisten / stayfriends:
Bayerisches Landesamt für Datenschutzaufsicht
in der Regierung von Mittelfranken; datenschutz@reg-mfr.bayern.de

partyface:
Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz; poststelle@datenschutz.rlp.de

Sie interessieren sich für das Thema

„Medienkompetenz und Datenschutz für Kinder und Jugendliche“?

Die Arbeitsgruppe „Schule/Bildung“ der Datenschutzbeauftragten des Bundes und der Länder hat eine Link-Liste mit empfehlenswerten Seiten zusammengestellt. Diese finden Sie im Internetangebot des Landesbeauftragten für den Datenschutz Rheinland-Pfalz (www.datenschutz.rlp.de) unter der Rubrik „Jugend - Aktuelles“.