# Sicher digital kommunizieren und zusammenarbeiten

## Datensicherheit für Engagierte und Organisationen im Netz

Von Larissa Aldehoff & Sarah Morcos

### Überblick

Datensicherheit ist sowohl für Organisationen als Ganzes als auch die Menschen, die sich engagieren, von größter Wichtigkeit. Das Sammeln von Daten ist alltäglich geworden. Deswegen muss unbedingt gewährleistet sein, dass diese Daten sicher kommuniziert und gespeichert werden, um Datenmissbrauch zu verhindern. Die wichtigsten gesetzlichen Grundlagen und einige Tipps zur Anwendung stellt diese MuP-Praxishilfe vor.

**Inhaltsverzeichnis**



### Sicher im Netz arbeiten: Datenschutz, Kommunikation und Vernetzung

NPO müssen immer auch das Thema digitale Sicherheit mitdenken! Erst wenn eine Organisation weiß, wie Sie Ihre Daten und Kommunikation schützen kann, können digitale Arbeitsweisen auch einen echten Mehrwert bringen!
Sensible und personenbezogene Daten[1] sollten generell so wenig wie möglich erhoben werden, was nicht festgehalten ist, kann auch nicht missbraucht werden. Die Daten, die erfasst sind, müssen unbedingt geschützt werden. Deswegen sollte es klare Regelungen geben, wie diese Daten geschützt werden und wer Zugang dazu bekommt.

**Virenschutz**: Virenschutzprogramme sind sehr bekannt. Diese gewährleisten allerdings keine vollständige Sicherheit und können mitunter sogar selbst Sicherheitslücken verursachen. Deswegen sind zwei Maßnahmen sehr viel wichtiger:

- Aktualisieren Sie Ihre Software regelmäßig, also immer, wenn Sie zu einem Update aufgefordert werden.
- Außerdem sind sogenannte Ad-Blocker sehr wichtig, kleine Programme, die Werbung auf Internetseiten blockieren. Diese ist nicht nur lästig, sondern kann auch im Falle von bspw. seriösen Nachrichtenportalen Viren enthalten, die sich auf Ihren PC übertragen. Weit verbreitet ist Ad-Blockplus, uBlock hat einen vergleichbaren Funktionsumfang, verbraucht aber wesentlich weniger Arbeitsspeicher.

**Passwörter**: Sie sollten für jede Anwendung ein eigenes Passwort setzen. Werden Datenbanken, in denen Passwörter gespeichert werden, gehackt, gerät Ihr universelles Passwort ansonsten sehr schnell in die falschen Hände.

**Für die Praxis:** Viele hilfreiche Infos, Beispiele und Empfehlungen für die Handhabe von Passwörtern finden Sie beim Projekt Verbraucher sicher online!

[1] Personenbezogen und also schutzwürdig sind Daten, die Rückschlüsse auf eine bestimme Person zulassen und die eine Organisation oder ein Verein für die Mitgliederverwaltung benötigt, also typischerweise: Name und Anschrift, Geburtsdatum, Eintrittsdatum, Bankverbindung

**Cloud-Dienste und Kollaborationsplattformen**: Bevor Sie sich für einen bestimmten Cloud-Dienst oder eine Kollaborationsplattform entscheiden, prüfen Sie deren Allgemeine Geschäftsbedingungen und Datenschutzbestimmungen. Anbieter, deren Server nicht in Deutschland liegen, unterliegen auch nicht deutschen Datenschutzbestimmungen. Außerdem gilt auch hier die Frage: Wer bekommt Zugang zu diesen Werkzeugen und damit zu den ausgetauschten Daten? Legen Sie generell keine sensiblen und personenbezogenen Daten in Clouds ab! Weitere Informationen bietet das Informationsportal iRIGHTS CLOUD, ein Informationsangebot speziell zu Cloud-Diensten der Informationsplattform und Online-Magazin iRights.info

**e-Mails:** E-Mails, die nicht in einem besonderen Verfahren verschlüsselt werden, sind sehr unsicher und können sehr leicht von außen gelesen werden. Auch hier sollte abgewogen werden, welche Daten überhaupt über eine virtuelle Postkarte verschickt werden dürfen.

**Für die Praxis**

Das Projekt „Verbraucher sicher online“ der Technischen Universität Berlin bietet praktische Empfehlungen und einen guten Überblick über Verschlüsselung von E-Mails.

**organisationsinterne Themen und Informationen:** Vertrauliche Informationen sollten auf keinen Fall in sozialen Netzwerken veröffentlicht werden, egal ob es um sensible Daten einer Organisation geht oder Interna auf Karriereportalen. Ansonsten drohen rechtliche Konsequenzen für Sie.

**respektvoller Umgang:** Bei Diskussionen in sozialen Medien gilt die Meinungsfreiheit, doch ebenso eine respektvolle, tolerante Diskussionskultur. Im Falle von strittigen Aussagen ist eine höfliche, aber eben auch bestimmte Moderation der Beiträge unbedingt erforderlich. Eine Netiquette kann sinnvoll sein, auf diese kann im Falle von beleidigenden Äußerungen, Hassrede etc. verwiesen werden. Ein Beispiel ist die Netiquette des Bundesministeriums für Familie, Senioren, Frauen und Jugend für Soziale Medien

**Hinweis** : Zum Umgang mit Beleidigungen oder antidemokratischen Aussagen bietet das **MuP-Thema im Fokus** „Rechtspopulisten Paroli bieten! Aktiv für Demokratie und Toleranz“ hilfreiche Anregungen!

**Recht und Gesetz**: Rechtswidrige Inhalte sind auch online strafbar – übrigens auch, wenn sie nicht öffentlich gepostet worden sind – und sollten unbedingt gemeldet werden. Im Extremfall kann rechtlicher Beistand zur Beratung herangezogen werden, sollte aber nicht in der Diskussion angedroht werden, sondern ausschließlich im Hintergrund agieren.

**Schutz sensibler Daten:** Niemals sensible Daten über soziale Netzwerke oder Messenger-Dienste kommunizieren!

**Auf den Punkt**

Egal auf welchem Weg Sie kommunizieren, kommunizieren Sie immer nur so viele Daten wie nötig und so sicher wie möglich. Je weniger Daten Sie in Nachrichten und Bildern verbreiten, desto geringer ist die Wahrscheinlichkeit, dass sie in die falschen Hände geraten.

**Fragen Sie in Ihrer Organisation:**

- ? Welche Daten braucht unsere Organisation wirklich?
- ? Wie können wir unsere Daten & Informationen schützen?
- ? Wie können wir die Daten, die uns Menschen anvertrauen, schützen?
- ? Über welche Kanäle kann man am sichersten kommunizieren?
- ? Wer bekommt den Zugang zu den Daten und den Werkzeugen der Datenverarbeitung?

## Sichere Internetpräsenz

Egal ob NPO, Parteien, Vereine, Initiativen, Verbände oder Gewerkschaften – nahezu 100 % aller Organisationen haben eine Präsenz im Internet. Hierbei sind einige wichtige Dinge unbedingt zu beachten! Denn auch hier gilt: Unwissenheit schützt vor Strafe nicht.

- ☑ **Verschlüsselung**: Werden auf der Internetseite Ihrer Organisation Daten abgefragt und gespeichert, sollte die Seite unbedingt verschlüsselt sein, dies ist zu erkennen an der Protokollbezeichnung https:// vor der Adresse. Auch ein passwortgeschützter interner Bereich für Mitglieder kann sinnvoll sein.

- ☑ **Server**: Es ist wichtig, dass Sie wissen, wo der Server Ihrer Internetseite liegt. Denn dieser Standort entscheidet darüber, welches Datenschutzrecht für Ihre Internetpräsenz gilt. Befindet sich der Server Ihrer Internetseite in Deutschland, gilt auch deutsches Datenschutzrecht. Das kann Ihre Situation erheblich erleichtern.

- ☑ **Urheber- und Persönlichkeitsrechte**: Beachten Sie unbedingt die Urheber- und Persönlichkeitsrechte, wenn Sie Texte, Bilder, Lieder und Videos auf Ihrer Internetseite, einem Blog oder in sozialen Medien veröffentlichen. Dies gilt übrigens auch für ausschließlich nach innen gerichtete Kommunikation! Um das Recht am eigenen Bild einzuhalten, müssen Sie außerdem Personen, die einzeln auf Fotos zu sehen sind, um Erlaubnis bitten, bevor Sie entsprechende Fotos veröffentlichen dürfen. Übertragen Sie einen Live-Stream, ist es besonders wichtig, die Rechte Dritter vorher zu klären. Alle Personen, die zu sehen sind, müssen vorher eingewilligt haben. Ansonsten drohen rechtliche Folgen.

  **Für die Praxis:**

  Eine interessante Einführung mit vielen weiteren hilfreichen Quellen und Links zu dem Thema hat Matthias Spielkamp im Artikel „Fremde Inhalte auf eigenen Seiten“ veröffentlicht.

  Informationsplattform und Online-Magazin **iRights.info** bietet konkrete Hilfen und Empfehlungen zu den Themen Datenschutz und Sicherheit sowie zu Creative Commons und Lizenzen.

- ☑ **Impressum**: Internetseiten müssen in Deutschland ein Impressum haben, das verdeutlicht, wer für die Seite und ihre Inhalte verantwortlich ist. Entsprechend muss jedes Impressum mindestens diese Angaben enthalten:
  - Name, Adresse, Telefonnummer, E-Mail-Adresse und falls vorhanden Faxnummer der Person, die die Internetseite betreibt sowie Vertretungsberechtigte_r der Organisation

- ☑ **Datenschutzerklärung**: Wenn Sie auf Ihrer Internetseite personenbezogene Daten verarbeiten, sind Sie gesetzlich dazu verpflichtet, die Seitenbesucher_innen darüber zu informieren, welche Daten erfasst und gespeichert werden und was damit passiert.

- ☑ **Schreibrechte**: Falls mehrere Menschen Schreibrechte für eine Internetseite oder Präsenz in sozialen Medien bekommen, sollte jede Person einen eigenen Zugang haben. Nur so bleibt nachvollziehbar, wer welchen Beitrag verfasst hat.

- ☑ **Cookies**: Cookies sind Textdateien, die Informationen über die Besucher_innen auf Ihrer Internetseite speichern. Diese helfen Ihnen, Inhalte (und möglicherweise Werbung) besser auf Ihre Zielgruppe zuzuschneiden. Die aktuelle Gesetzeslage zwingt Seitenbetreiber_innen zwar nicht, die Nutzung von Cookies offen zu legen, es ist aber dennoch empfehlenswert, Seitenbesucher_innen darauf hinzuweisen, so dass diese sie ggf. deaktivieren können.

- ☑ **Datenerhebung nur anonymisiert**: Mit Tracking verfolgt man, welche_r Besucher_in welche Teile der Internetseite aufgerufen hat. Targeting analysiert das individuelle Verhalten der Besucher_innen, um zielgruppengerechte Werbung schalten zu können.
  Diese Verfahren sind in Deutschland erlaubt, allerdings nur, wenn die erfassten Daten und alle weiteren Informationen anonymisiert werden.

**Auf den Punkt: Sicheres Engagement durch:**

- **Datensparsamkeit**: Engagierte und NPO sollten immer nach dem Grundsatz der Datensparsamkeit handeln und kommunizieren.
- **Kompetenzbildung**: Auch wenn es im oft hektischen Alltag schwer fallen mag – die Weiterbildung von Haupt- und Ehrenamtlichen ist unabdingbar für wirklich sicheres Arbeiten und Kommunizieren im Internet.
- **Gemeinsames Sicherheitsbewusstsein**: Mit den entsprechenden Kompetenzen entwickeln sich auch das nötige Bewusstsein und die Akzeptanz für eine Sicherheitsstrategie. Denn nur wenn alle Beteiligten in einer Organisation zusammen die Sicherheitsvorkehrungen einhalten, können diese auch funktionieren.

## Quellen und Verweise

- ❖ Mehr zum **Thema im Fokus** „Digitalisierung und Engagement“ finden Sie bei den Themen im Fokus auf unserer MuP-Website.

- ❖ Zu diesem Thema empfehlen wir Ihnen auch die **MuP-Praxishilfe** „Chancen der Digitalisierung für Engagement entdecken“! Sowie das **MuP-Interview** „Mehr Anerkennung für digitales Engagement“ mit Julian Fischer von der Wikimedia Deutschland und im **MuP-Interview** „Digitales Engagement mit offenen Daten und Civic Tech“ gibt Julia Kloiber einen Einblick in ihre Praxis und erklärt, warum offene Daten wichtig für eine starke Zivilgesellschaft sind.

- ❖ Quelle: Online-Dossiers „Ehrenamtlich Aktive sicher im Netz“ und Pädagogik und Didaktik“ von Digitale Nachbarschaft, ein Projekt des Vereins **Deutschland sicher im Netz**.