Was ist drin in diesem Ratgeber?

1. Rechtliche Grundlagen

Das **Grundgesetz** gibt uns in Deutschland das Recht auf eine freie Entfaltung, auf Meinungs- und Pressefreiheit.

Zusätzlich hat das Bundesverfassungsgericht weitere wichtige Grundrechte für unsere eigenen Daten und für unsere Rechte auf eine persönliche und freie Entfaltung im Zusammenhang mit Computern und Internet definiert:

Das **Recht auf Informationelle Selbstbestimmung** bezeichnet das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen (seit 1983).

Das **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme** (umgangssprachlich auch als **IT-Grundrecht**, **Computer-Grundrecht** oder **Grundrecht auf digitale Intimsphäre** bezeichnet) ist ein deutsches Grundrecht, welches vornehmlich dem Schutz von persönlichen Daten dient, die in Computern, Rechnern und Servern gespeichert oder verarbeitet werden (seit 2008).

Und in der Europäischen Menschenrechtskonvention steht:

"Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs."

Ohne Internet geht (fast) gar nichts mehr.

Ganz egal, ob man diese Tatsache nun gut findet oder nicht - es lässt sich nicht ändern.

Bei aller Kritik, Sorge und Gefährdung darf aber auch nicht vergessen werden, welche Vorteile das Internet bringt oder bringen kann:

Informationsaustausch rund um die Uhr, Kennenlernen von Freunden und interessanten Menschen und Projekten, kritische Meinungsverbreitung, unglaublich viele Gestaltungs- und Ausdrucksmöglichkeiten.

Für manche Menschen ist es z.B, ein großer Vorteil, in Chats und Foren anonym Fragen stellen zu können, die man die Eltern, Freunde oder Ärzte nicht zu stellen wagen würde.

Damit das auch so bleibt, müssen heutzutage leider einige "Spielregeln" beachtet werden.

Denn genauso wirtschaftliche Akteure wie auch staatliche und private Interessengruppen haben ein großes Interesse an unseren privaten Daten über Konsum- und Surfverhalten, unsere Kommunikationsmuster, unsere sozialen Netzwerke, politische Aktivitäten, biometrische Daten usw. usw. !

Diese Informationen können z.B. durch Banken, Krankenkassen, Versicherungen, Behörden und Arbeitgeber gegen unseren Willen und ohne unser Wissen gegen uns verwendet werden!

Deswegen dieser Ratgeber!

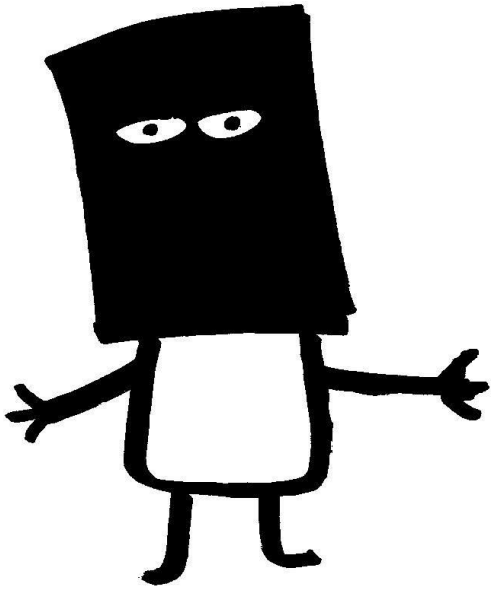
Herausgeber dieses Blattes:

AK Vorrat, Ortsgruppe Hannover
Stand: Mai 2009
http://wiki.vorratsdatenspeicherung.de/Hannover

Mehr Infos zum Arbeitskreis Vorratsdatenspeicherung:
www.vorratsdatenspeicherung.de

V.i.S.d.P.
Michael Ebeling, Kochstraße 6, 30451 Hannover,
micha_ebeling@gmx.de

AK VORRAT hannover



Anonym und sicher im Internet

Ein Ratgeber

2. Grundsätzliches: Umgang mit persönlichen Daten

Wichtig ist vor allem:

Das Internet vergisst NICHTS!

Das bedeutet zum Beispiel:

Auch in zehn oder zwanzig Jahren sind deine Äußerungen und Sprüche in Foren zu sehen!
Auch wenn sich deine Meinung inzwischen vielleicht geändert hat!

Dann wird man immer noch nachsehen können, welche Fotos du hochgeladen hast oder welche Fotos über dich hochgeladen worden sind.

Deswegen ist es wichtig, sich das immer wieder klar zu machen, bevor man etwas in die Internet-Welt schreibt.

Ratschläge:

- Gehe sparsam und vorsichtig mit deinen Daten und Meinungen um.
- Sei kritisch und vorsichtig! Zum Beispiel, wenn irgend jemand im Internet (z.B. bei der Anmeldung in Foren oder bei Firmen) etwas von dir wissen will, was ihn eigentlich gar nichts angeht.
- Nutze das umfangreiche und kostenlose OpenSource-Betriebssystem Ubuntu statt MicrosoftWindows.
- Verwende einen OpenSource-Browser (z.B. Firefox) und nicht den unsicheren InternetExplorer
- Halte deinen Browser durch Updates auf dem Laufenden.
- Sei vorsichtig mit Cookies und JavaScript!
- Verwende verschiedene Nicknames und ändere diese Namen und deine Passwörter ab und zu.
- Lass dir trotzdem dem Spaß am Internet nicht verderben!

Links/Hinweise:

- Zeigt, wo wir heutzutage überall Datenspuren hinterlassen: http://panopti.com.onreact.com/
- Firefox - ein "freier" und potentiell sicherer Browser: http://www.mozilla-europe.org/de/firefox/
- Das Bundesamt für Sicherheit in der Informationstechnik: http://www.bsi-fuer-buerger.de/
- http://www.ubuntuusers.de – hier gibt es alles an Beratung und Informationen zu „Ubuntu“

3. Anonym surfen

Anonym surfen bedeutet, dass die Seite, die du anwählst, nicht erkennen kann, wer du bist und wo du dich befindest.

Hierzu gibt es einige "Anonymisierungs-Dienste", die allerdings längst nicht alle gut oder schnell oder kostenlos sind.

Außerdem müssen alle in Deutschland sitzenden "Anonymisierer" aufgrund des Gesetzes zur Vorratsdatenspeicherung trotzdem speichern, wann du dir welche Seiten angesehen hast.

(Übrigens: Gegen dieses Gesetz, dass seit 2008 auch dafür sorgt, dass gespeichert werden muss, wann und mit wem und wie lange und von wo du telefoniert hast, haben "wir" - der Arbeitskreis Vorratsdatenspeicherung - eine Verfassungsbeschwerde eingelegt, an der sich mehr als 34000 Bürger beteiligt haben!)

Ratschläge:

- Überlege ab und zu, ob es dir lieb ist, dass (theoretisch jeder andere Mensch) zusehen kann, auf welchen Seiten du dich aufhältst und was du dir im Internet so ansiehst.
- Verwende eine Anonymisierungs-Software zumindest in den Momenten im Internet, an denen es dir wichtig erscheint.
- Deaktiviere Cookies oder lasse sie und deine persönlichen Daten automatisch löschen, sobald du deinen Browser schließt (kann man bei Firefox so einstellen!)
- Gib dein Wissen an Freunde und Bekannte weiter.

Links/Hinweise:

- Tor - eine kostenloser Anonymisierdienst: https://www.torproject.org/
- I2P - ein weiterer kostenloser Anonymisierungsdienst: http://www.i2p2.de/index_de
- Suchmaschinen, die dein Suchverhalten NICHT speichern und diese Informationen weiterverkaufen: www.scroogle.de oder www.ixquick.de

4. Sicher Kommunizieren

Im Normalfall kann "jeder" alles das sehen und lesen, was du per E-Mail schreibst, welche Passwörter du eingibst, und welche Daten du in Internet-Formularen eingibst.

Um das verhindern, solltest du beim Senden von Passwörtern und Daten immer darauf achten, dass oben im Browser eine Verbindung mit "https://" steht. Dann werden die Daten nämlich verschlüsselt und sind durch Dritte nicht ohne weiteres einsehbar.
Probiere es aus: Meistens muss man selber daran denken und dafür sorgen, dass man nicht mit der unsicheren "http://"-Verbindung am Surfen ist!

E-Mails zu verschlüsseln wird für viele Menschen immer selbstverständlicher. Dafür hat sich PGP (Pretty Good Privacy) als Open-Source-Programm quasi als Standard durchgesetzt.

Ratschläge:

- Verwende eine sichere Anwendung für deine E-Mail-Verwaltung, also z.B. Thunderbird (kostenlos und OpenSource) statt Outlook.
- Verschlüssele deine E-Mails, damit sie nicht von anderen gelesen werden können.
- Verwende sichere https-Verbindungen bei der Übermittlung von persönlichen Daten.
- Statte den Firefox-Browser mit Sicherheits-AddOns aus, damit dir keiner über die Schultern schaut (BetterPrivacy, NoScript, Stealther, Adblock Plus, Cookiesafe, Flashblock und Ghostery)
- Verwende Antivirenprogramme und Anti-Spy-Tools

Links/Hinweise:

- Thunderbird - kostenloser E-Mail-Client, der auch leicht die Einbindung von E-Mail-Verschlüsselung ermöglicht : http://www.mozilla-europe.org/de/products/thunderbird/
- Reclaim-Your-Computer-Projekt - mit Anleitungen und Tips http://reclaimyourcomputer.toxisch.net/
- TrueCrypt - kostenlose und extrem sichere Verschlüsselung von Festplatten und USB-Sticks: http://www.truecrypt.org/
- Hier gibt es kostenlose und anonyme Einweg-E-Mail-Adressen zum anonymen Anmelden in Internetportalen: www.anonbox.net