Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB
Préposé fédéral à la protection des données et à la transparence PFPDT
Incaricato federale della protezione dei dati e della trasparenza IFPDT
Incumbensà federal per la protecziun da datas e per la transparenza IFPDT

JUGEND UND MEDIEN
NATIONALE PLATTFORM ZUR FÖRDERUNG VON MEDIENKOMPETENZEN

Datenschutz

Informationsdossier

In Zusammenarbeit mit dem Eidg. Datenschutz- und Öffentlichkeitsbeauftragten EDÖB und der nationalen Plattform zur Förderung von Medienkompetenzen „Jugend und Medien" des Bundesamts für Sozialversicherungen BSV.

Inhaltsverzeichnis

1. Was ist Datenschutz?

Wenn wir im Klassenchat auf WhatsApp unsere Hausaufgaben besprechen oder auf Instagram ein neues Selfie posten, wenn wir krank sind und dies unserem Lehrer per E-Mail oder SMS ausrichten, wenn wir in einem Onlineshop ein Paar neue Sneakers bestellen oder auf der Strasse zur Teilnahme eines Wettbewerbs gebeten werden, bei dem wir Alter und Adresse angeben müssen – im Alltag werden viele persönliche Informationen ausgetauscht, und zwar nicht nur innerhalb der Familie und unter Freunden. Dass diese Daten auch in fremde Hände gelangen können und nicht immer so verwendet werden, wie wir das gerne möchten, sollten wir uns immer bewusst sein.

1.1. Definition

Der Begriff Datenschutz ist in der zweiten Hälfte des 20. Jahrhunderts entstanden und wird als Schutz der Privatsphäre bei der Datenverarbeitung und als Schutz des Rechts auf informationelle Selbstbestimmung definiert. Das bedeutet, dass jeder Mensch frei für sich entscheiden kann, welche seiner Personendaten wem zugänglich sein sollen und zu welchem Zweck sie verwendet werden dürfen.

Unter Personendaten verstehen wir alle Informationen, welche einer Person zugeordnet werden können, also zum Beispiel:

- Adressdaten
- Alter
- Persönliche Interessen und Neigungen
- Standortdaten, welche ein Handy via GPS aufzeichnet
- Eigenes Bild (z.B. Profilfoto)
- Etc.

Datenschutz bedeutet, dass die Privatsphäre der Menschen, deren Daten von Behörden, Unternehmen oder Privaten bearbeitet werden, geschützt wird.

Datenschutz wird in der zunehmend digitalen und vernetzten Informationsgesellschaft immer wichtiger. Er soll das unkontrollierte Sammeln und den Missbrauch von Daten verhindern und der Tendenz zum «gläsernen Menschen», der Entstehung von Datenmonopolen von Privatunternehmen sowie dem Ausufern staatlicher Überwachungsmassnahmen entgegen wirken.

(Quelle: Wikipedia)

Schutz der Person

Der Begriff Datenschutz mag eher trocken und unpersönlich klingen. Es geht dabei aber vor allem um uns selber, d.h. den Schutz unserer Persönlichkeit und unserer Grundrechte. Denn: Nicht alle Informationen über uns und unser Leben gehen jeden etwas an.

Alle Daten, die etwas mit uns zu tun haben, sind «personenbezogene Daten» oder «Personendaten». Diese Daten verraten viel über uns und sind kostbar. Für Unternehmen bedeuten sie bares Geld, und sie können von anderen missbraucht werden. Deshalb müssen wir sehr sorgfältig, d.h. sparsam und gut überlegt, mit unseren persönlichen Daten

umgehen. Wir müssen uns des Werts unserer Daten bewusst sein. Schützen wir unsere Daten, heisst das **Privatsphäre, Anonymität und mehr Sicherheit** für uns.

Besonders schützenswerte Daten

Gewisse Personendaten gelten als besonders schützenswert, weil es für die betroffenen Personen sehr negative Konsequenzen haben kann, wenn diese Informationen in falsche Hände gelangen. Als besonders schützenswerte Personendaten gelten u.a. Daten über die religiösen, weltanschaulichen, politischen Ansichten einer Person. Ausserdem auch Informationen zur Gesundheit, zur Intimsphäre (z.B. Sexualität) oder zu strafrechtlichen Verfolgungen und Sanktionen.

Die vollständige Auflistung findet sich unten unter «*1.1.1 Gesetzliche Grundlagen*».

Weiterführende Gedanken

Die heutige Technik ermöglicht ein beinahe unbeschränktes Erfassen, Zusammenführen, und Verfügen über Informationen. Dementsprechend ist auch das Potenzial für Persönlichkeitsverletzungen angewachsen. Als Einzelperson ist man kaum mehr in der Lage zu kontrollieren, wer welche Daten über einen bearbeitet. Tagtäglich geben wir Daten von uns, freiwillig oder unfreiwillig, an Drittpersonen weiter, oft ohne zu wissen, wozu sie genau verwendet werden oder wo und wie lange sie gespeichert werden. So können Unternehmen heute beispielsweise in Erfahrung bringen, ob ein Kunde ein guter oder schlechter Zahler ist, welche Bücher er liest oder welche Musik er hört, ohne dass die betroffenen Personen sich dessen bewusst sind.

Wenn Informationen über Menschen gesammelt und bearbeitet werden, ist deren Persönlichkeit davon betroffen. Die Betroffenheit kann stärker oder schwächer sein und positive oder negative Reaktionen hervorrufen. Eine Person kann ein Leben lang mit einem Makel behaftet bleiben, wenn Daten mit negativen Angaben über sie auf unbestimmte Zeit aufbewahrt und immer wieder benutzt werden. Deshalb sind Personendaten ein schützenswertes Gut. Für die betroffene Person selbst, als auch für Drittpersonen, die ein Interesse daran haben.

Ziel des Datenschutzes ist es, dieses wertvolle Gut zu schützen: Er setzt Leitplanken für die Bearbeitung von Personendaten, um zu garantieren, dass die Entfaltung der Persönlichkeit nicht durch unerwünschte Datenbearbeitungen beeinträchtigt wird. Jedermann soll, soweit die Rechtsordnung nichts Anderes vorsieht, selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen. *(vgl. Botschaft zum Bundesgesetz über den Datenschutz, DSG, 23. März 1988, Ziff. 113: Allgemeine Ziele eines Datenschutzgesetzes)*

Jede Person hat zudem das Recht zu erfahren, wer was über einen weiss und zu welchen Zwecken die entsprechenden Daten bearbeitet werden. Wir können vom Inhaber einer Datensammlung die Herausgabe unserer persönlichen Daten verlangen, diese korrigieren oder löschen lassen.

Darum ist Datenschutz wichtig

Die **Informationstechnologie** ermöglicht, enorme **Mengen von Personendaten zu erfassen und miteinander in Verbindung zu setzen** (Stichworte: Big Data, künstliche Intelligenz, Internet of Things). Oft hält das Sicherheitsbewusstsein der Datenbearbeiter nicht mit den technischen Neuerungen Schritt. Zudem sind die meisten Menschen – seien es die Bearbeiter von Daten, seien es die Personen, deren Daten bearbeitet werden – noch nicht genügend für Fragen des Persönlichkeitsschutzes sensibilisiert.

Viele Menschen gehen sehr leichtfertig mit ihren persönlichen Daten um, sei es im Internet, sei es beim Ausfüllen von **Umfrage- und Wettbewerbsformularen** oder auch bei der Verwendung **diverser Apps auf unserem Smartphone** (Aktivierung der Standortfunktion, Preisgabe persönlicher Informationen in sozialen Netzwerken etc.), um nur einige Beispiele zu nennen.

Nicht nur wegen den zunehmenden technischen Möglichkeiten und den damit einhergehenden Risiken (Datenverlust, Identitätsdiebstahl etc.) braucht es Leitplanken zum Schutz der Privatsphäre. Auch zur Ausübung von Freiheitsrechten wie Meinungsäusserungsfreiheit, Glaubensfreiheit und Versammlungsfreiheit ist der Datenschutz Voraussetzung.

Denn: Würden Sie Ihre Meinung noch frei äussern, wenn Sie befürchten müssten, abgehört zu werden? Wie würden Sie stimmen und wählen, wenn Sie dies öffentlich und unter Namensnennung tun müssten?

Der **Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB)** sorgt dafür, dass die im Datenschutzgesetz verankerten Leitplanken eingehalten werden. Ausserdem berät er Privatpersonen und Bundesorgane im Hinblick auf die Einhaltung der gesetzlichen Datenschutzbestimmungen. Der EDÖB soll also informieren und sensibilisieren, aber auch einschreiten, wenn Inhaber von Datensammlungen die Grundsätze des Datenschutzes nicht einhalten.

(siehe auch https://www.edoeb.admin.ch/edoeb/de/home/der-edoeb/auftrag.html)

1.1.1. Gesetzliche Grundlagen

Europäische Menschenrechtskonvention (EMRK)

Art. 8 Recht auf Achtung des Privat- und Familienlebens

[1] Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.

[2] Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.

Datenschutz in der Bundesverfassung:

Art. 13 Schutz der Privatsphäre

[1] Jede Person hat Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs.

[2] Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.

Der Datenschutz ist also dazu da, die Informationen zu einzelnen Personen zu schützen. Jeder Mensch hat das Recht, selbst zu bestimmen, welche Informationen über ihn wann, wo und wem bekanntgegeben werden. Der Datenschutz achtet darauf, dass immer nur so viele persönliche Daten wie nötig und so wenig persönliche Daten wie möglich gesammelt und bearbeitet werden. Jeder Mensch hat zudem das Recht Einsicht in die Daten zu erhalten, welche über ihn erfasst werden.

Schweizerisches Zivilgesetzbuch (ZGB)

Art. 281B. Schutz der Persönlichkeit / II. Gegen Verletzungen / 1. Grundsatz

II. Gegen Verletzungen

1. Grundsatz

[1] Wer in seiner Persönlichkeit widerrechtlich verletzt wird, kann zu seinem Schutz gegen jeden, der an der Verletzung mitwirkt, das Gericht anrufen.

[2] Eine Verletzung ist widerrechtlich, wenn sie nicht durch Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist.

Siehe ausserdem: Art. 28a ff. ZGB (Schutz der Persönlichkeit).
https://www.admin.ch/opc/de/classified-compilation/19070042/index.html#a28a

Bundesgesetz über den Datenschutz (DSG):

Art. 1 Zweck

Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden.

(…)

Art. 4 Grundsätze

[1] Personendaten dürfen nur **rechtmässig bearbeitet** werden.

[2] Ihre Bearbeitung hat **nach Treu und Glauben** zu erfolgen und muss verhältnismässig sein.

[3] Personendaten dürfen nur **zu dem Zweck** bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.

[4] Die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung müssen für die betroffene Person **erkennbar** sein.

[5] Ist für die Bearbeitung von Personendaten die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung erst gültig, wenn sie nach **angemessener Information freiwillig** erfolgt. Bei der Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen muss die Einwilligung zudem ausdrücklich erfolgen.

Besonders schützenswerte Daten im Bundesgesetz über den Datenschutz

Art. 3 Begriffe

c. besonders schützenswerte Personendaten:
Daten über:
1. die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten,
2. die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit,
3. Massnahmen der sozialen Hilfe,
4. administrative oder strafrechtliche Verfolgungen und Sanktionen

Anpassung im neuen Datenschutzgesetz

Im neuen Datenschutzgesetz (DSG) sollen, neben den bisherigen, auch biometrische und genetische Daten sowie Persönlichkeitsprofile als besonders schützenswerte Personendaten gelten.

1.1.2. Fazit

In Anbetracht der erwähnten technologischen Fortschritte und den damit verbundenen Möglichkeiten, Personendaten schneller und in grösseren Mengen zu speichern und miteinander in Verbindung zu setzen, ist es unerlässlich, sich mit dem Datenschutz auseinanderzusetzen.

Gerade mit den Möglichkeiten, welche das Internet bietet, sind Daten schnell für Drittpersonen zugänglich, und was einmal «online» ist, kann nur schwer oder gar nicht mehr vollständig gelöscht oder berichtigt werden. Das Internet vergisst nicht.

Wichtig ist insbesondere, dass man als Privatperson seine Rechte kennt und weiss, wie man selber aktiv werden kann, sollten die eigenen Personendaten zu Unrecht gespeichert, verarbeitet oder weitergegeben werden. Dabei sollen das vorliegende Informationsdossier und die damit verbundenen Arbeitsblätter und Aufträge helfen.

Ausserdem ist es von zentraler Bedeutung, dass man selbst die Richtlinien des Datenschutzes einhält, bewusst mit eigenen und korrekt mit fremden (Personen-) Daten umgeht. Hierfür finden sich in Kapitel 3 «Tipps für den richtigen Umgang mit Daten» konkrete Handlungshinweise und Tipps.

1.2. Wer hat ein Interesse an Personendaten? Wer sammelt sie und warum?

Es gibt verschiedene Gründe, weshalb jemand Interesse an unseren Daten bekundet.

1.2.1. Staatliche Datensammlung

Vor allem in autoritären und totalitären Staaten haben die staatlichen Behörden selbst ein Interesse daran zu wissen, wie sich ihre Bürger verhalten. Hier ist das Ziel, Kontrolle über die Bürgerinnen und Bürger zu erlangen (Stichwort: «gläserner Bürger»).
Ein besonders gravierendes Beispiel war die gesellschaftliche **Überwachung** im nationalsozialistischen Deutschland von 1933 bis 1945. Es wurden Listen über politische Feinde im Allgemeinen und Juden im Besonderen erstellt. Das Ziel war nebst der Absicherung der Macht der Nationalsozialisten die totale Vernichtung der Juden. Der Judenstern – Juden mussten ihre Zugehörigkeit zum jüdischen Glauben durch einen aufgenähten Stern jederzeit vorzeigen – war ein besonders «sichtbarer» Verstoss gegen das heutige Verständnis von Datenschutz.

Auch in demokratischen Ländern wie der Schweiz werden Daten gesammelt, Leute beobachtet und überwacht. In den späten 1980er-Jahren kam ans Tageslicht, dass die Schweizer Bundesbehörden und die kantonalen Polizeibehörden rund 700`000 Fichen (Karteikarten) angelegt und damit sensible Daten und weltanschauliche Informationen über rund 10% der Schweizer Bürgerinnen und Bürger gesammelt hatten. Offizielles Ziel war es, das Land vor der «Gefahr des Kommunismus» zu schützen. Folge des sogenannten **Fichen-Skandals** war, dass das Vertrauen der Bürgerinnen und Bürger in den Staat für längere Zeit erschüttert war.
Aber auch heute werden Daten von Behörden gesammelt, offiziell und legal. Zum Beispiel werden in der Schweiz Mitglieder extremistischer und krimineller Gruppierungen oder

Menschen mit Verbindungen zum internationalen Terrorismus überwacht. Diese Aufgabe erfüllt der Nachrichtendienst des Bundes (NDB), der dem Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) unterstellt ist.
Selbstverständlich darf in einem Rechtsstaat jemand nicht grundlos überwacht werden. Es bestehen enge gesetzliche Grundlagen, die einen solchen Eingriff in die persönlichen Rechte regeln. Staatliches Handeln muss also **in einem Gesetz vorgesehen** sein (z. B. Strafprozessrecht, Nachrichtendienstgesetz). Man spricht vom Prinzip der **Rechtmässigkeit**).
Bei Untersuchungen, Ermittlungen und der Überwachung von Personen gilt zudem das Prinzip der **Verhältnismässigkeit**. Es muss in jedem Fall abgewogen werden, ob der Einschnitt in private Interesse und Grundrechte durch das allgemeine öffentliche Interesse gerechtfertigt ist.

Rechtmässigkeit und Verhältnismässigkeit in der Bundesverfassung (BV):

Art. 5 Grundsätze rechtstaatlichen Handelns

[1] Grundlage und Schranke staatlichen Handelns ist das Recht.

[2] Staatliches Handeln muss im öffentlichen Interesse liegen und verhältnismässig sein.

1.2.2. Datensammlung von Privaten und Firmen

Internetanbieter und Onlinedienste

Wer Internetdienste nutzt, sei es mit dem Computer, dem Tablet oder dem Mobiltelefon, generiert automatisch Daten. Diese Daten können durch die Internetanbieter gespeichert werden. So kann festgestellt werden, wer wie lange auf welcher Interseite surft oder welche App genutzt wird. Diese Daten sind für Unternehmen interessant und aufschlussreich, da sie unter anderem über das Konsumverhalten und die Vorlieben der Internetnutzer Auskunft geben. Dementsprechend kann dem Nutzer z. B. auch personalisierte Werbung, zugeschnitten auf seine Interessen, zugespielt werden. Wer sich öfters auf Online-Shoppingportalen und in Shopping-Apps aufhält, findet dementsprechend im Browser oder direkt in der App eventuell Vorschläge, was ihm oder ihr ausserdem noch gefallen könnte.

Versicherungen

Anhand von Statistiken, die in der Regel mit anonymisierten Daten auskommen, können Risikogruppen definiert und dementsprechend für einzelne Gruppen höhere Versicherungsprämien verlangt werden. Dies ist beispielsweise bei Statistiken über Verkehrsunfälle der Fall: Je nach Alter oder Geschlecht bezahlen gewissen Kategorien von Versicherten höhere Prämien als andere Versicherte, weil ihre «Gruppe» statistisch mehr Unfälle verursacht, dafür bezahlen sie bei der Krankenkasse weniger, weil sie in der Regel weniger krank sind.

Zur Ermittlung von massgeschneiderten Versicherungsmodellen oder zur Teilnahme an Bonusprogrammen sammeln Versicherungen aber vermehrt persönliche Informationen, darunter auch besonders schützenswerte Daten zur Gesundheit oder Bewegungsprofile.

Detailhändler

Kundenprofile helfen den Detailhändlern, das Kaufverhalten ihrer Kundinnen und Kunden zu analysieren. Dadurch können sie ihr Warenangebot und die Werbung gezielt darauf ausrichten, mehr Umsatz und mehr Gewinn zu erzielen. Der Käufer läuft Gefahr, indirekt manipuliert zu werden.

Umfrage- und Wettbewerbsformulare

Meist bilden diese Formulare die Basis, mit deren Hilfe Firmen ihre Werbung personalisieren und an potenzielle Kundinnen und Kunden adressieren können.

Adressen und andere persönliche Daten sind für ein effizientes Direktmarketing von grosser Bedeutung. Mit Hilfe möglichst genauer Informationen über Alter, Beruf, Konsumverhalten usw. kann das Risiko vergeblicher Werbung minimiert werden. In der Bevölkerung gibt es eine grosse Bereitschaft zur Auskunftserteilung. Selbst intime Daten werden preisgegeben, wenn die Befragten meinen, sie würden ihre Daten für ein wissenschaftliches Projekt zur Verfügung stellen. Besonders ergiebig scheint es zu sein, solche Umfragen in Verbindung mit der Teilnahme an einem Wettbewerb oder einem Gewinnspiel durchzuführen, bei dem der Zweck der Datenerhebung nicht klar ersichtlich ist. Meist steht nur im Kleingedruckten, dass die Daten für weitere Zwecke verwendet werden, was oft übersehen wird. Somit werden potenzielle Kunden veranlasst, ihre Daten herauszugeben. Verdeckte kommerzielle Datenerhebungen sind unzulässig.

Kredit-, Wirtschafts- und Handelsauskunfteien

Auskunfteien sammeln Informationen von Personen, die eine Rechnung nicht rechtzeitig bezahlen, einen Zahlungsbefehl bekommen oder eine Betreibung erhalten, und stufen sie als nicht kreditwürdig ein – auch wenn sich das Ganze manchmal als Missverständnis herausstellt. Es kann dann passieren, dass einer Person beispielsweise der Abschluss eines Handy-Vertrags verweigert wird oder ein Versandhandel nur bereit ist, gegen Nachnahme zu liefern.

Eine weitere Stelle, die Informationen über Zahlungsgewohnheiten besitzen, sind sogenannte Inkassobüros. Es handelt sich hierbei um private Unternehmen, die offene Rechnungen eintreiben. Oft werden Auskunftei- und Inkassodienste vom selben Unternehmen angeboten.

Die Daten in diesen Sammlungen umfassen nebst Angaben zum Schuldner unter anderem auch Daten über die Art der Schuld, von wann sie datiert und wie hoch der Betrag ist. Die Angaben stammen aus verschiedenen Quellen, die beispielsweise im Internet öffentlich zugänglich sind. Vor Abschluss eines Vertrages können Interessierte bei der Kreditauskunftei anfragen, ob ein zukünftiger Vertragspartner kreditwürdig ist und seinen finanziellen Verpflichtungen nachkommt.

Wenn die Angaben falsch sind, kann der Betroffene die Löschung bzw. Berichtigung verlangen.

2. Moderne Informationstechnologien und ihre Risiken

2.1. Internet und Computer

2.1.1. Web 2.0 – eine Idee mit vielen Fallen

Menschen, die sich im Internet bewegen, sind seit einigen Jahren nicht mehr nur «Konsumenten», sondern nutzen das Internet immer häufiger, um Informationen, Fotos, Videos etc. zu verbreiten. Internetseiten werden dynamischer und interaktiver. Im Fachjargon nennt man diese Entwicklung **Web 2.0**.

Immer wichtiger werden sogenannte «Soziale Netzwerke» oder auf Englisch «Social Networking Sites» (SNS).

Der Benutzer von solchen Internetportalen erstellt meist ein Profil, das Adressangaben, Vorlieben, Bilder und weitere Informationen und Daten enthält. Je nachdem, wie man die Einstellungen wählt, ist dieses Profil für alle Internetbesucher zugänglich. In der Regel sind die vorgegebenen Standarteinstellungen so gesetzt, dass man als Nutzer automatisch zu viele Daten von sich preisgibt, sofern dies nicht nachträglich geändert wird. Deshalb sollte man die Privatsphäre-Einstellung bei jedem Dienst prüfen und individuell anpassen. Teilweise muss man Rechte vergeben, sodass nur eine bestimmte Personengruppe Zugriff auf das Profil erhält. Aber oftmals gibt man mit den Standard-Einstellungen sehr viele persönliche Informationen über sich preis, ohne sich dessen bewusst zu sein.

Dadurch, dass die Internetbenutzer viele Informationen über sich selbständig und freiwillig veröffentlichen, wird der Datenschutz vor neue Herausforderungen gestellt. Wenn wir Informationen über andere Personen ungefragt ins Netz stellen, verletzen wir deren Privatsphäre und verstossen gegen das Datenschutzgesetz.

Aus Datenschutzsicht gibt es folgende Punkte zu beachten:

- Eine Vielzahl von ehemals als persönlich oder privat angesehenen Daten wird durch die SNS-Teilnehmer freiwillig einer breiten Öffentlichkeit präsentiert.
- Privatpersonen, Unternehmen, Regierungsstellen etc. erhalten somit einfach und anonym Zugriff auf persönliche Daten.
- Die Teilnehmer können auch Daten von Nichtmitgliedern auf SNS hochladen. Diese Daten werden somit ebenfalls der Öffentlichkeit zur weiteren Bearbeitung zugänglich gemacht.

Daraus ergeben sich verschiedene **Risiken**, denen ein User solcher Plattformen ausgesetzt ist:

- **Das Internet kennt kein Vergessen**. Benutzerprofile können von anderen Usern heruntergeladen und gespeichert werden, was die Löschung des Ursprungsprofils quasi nutzlos macht, bleiben die Daten doch erhalten. So entsteht eine Unzahl von privaten Datensammlungen und die Gefahr wächst, dass die Daten anders eingesetzt werden könnten als ursprünglich beabsichtigt.
- Die SNS-Provider haben nicht nur Zugriff auf Personendaten, sondern auch auf sogenannte Randdaten wie: Zeitpunkt des Login und Verbindungsdauer, geografische Herkunft der IP-Adresse, Verweildauer, Bewegungen auf der Seite etc.

- Bei vielen SNS-Anbieter ist unklar, was mit all diesen Daten geschieht. Klar ist: Personen- und Zusatzdaten zusammen können ausführliche Persönlichkeitsprofile ergeben, deren Verkauf grosse Gewinne abwerfen dürfte und deren Verwendung für die betroffenen Personen nachteilig sein können.
- **Automatisierte Gesichtserkennung**: Auf Facebook, Instagram, Google+ und ähnlichen Plattformen können Mitglieder Freunde und Bekannte auf Fotos markieren (taggen). Bei der automatisierten Gesichtserkennung scannt das System jedes neue Bild auf bereits bekannte und getaggte Freunde eines Nutzers und macht dann einen Namensvorschlag. In diesem Fall genügt ein Klick und der Freund ist fortan auf allen Fotos, auf denen er abgebildet ist, namentlich markiert. Das Feature ist bei manchen Plattformen automatisch eingeschaltet; wer nicht möchte, dass er getaggt wird, muss dies aktiv in den Privatsphären-Einstellungen vornehmen.
- In eine ähnliche Richtung geht die folgende Gefahr: Die automatische **Wiedererkennung** von Merkmalen im Hintergrund eines Bildes. Zur geografischen Lokalisierung eines Fotos können z. B. Landschaften oder Häuser im Hintergrund genutzt werden. Noch einfacher kann man ein Foto anhand der gespeicherten Metadaten einem Ort und Zeitpunkt zuordnen. Metadaten sind zusätzliche Informationen, welche in der Bilddatei gespeichert werden, z. B. Standortinformationen der Aufnahme, Datum und Uhrzeit der Aufnahme.
- Einige Plattformen erlauben das Hochladen auch von Daten von Drittpersonen - die keine Mitglieder des Netzwerkes sind – wohlgemerkt ohne deren Erlaubnis einzuholen. Dies kann zur Gefahr für die Privatsphäre der betroffenen Personen werden oder zumindest nicht in deren Interesse sein.
- Benutzerkonten können praktisch nicht unwiderruflich gelöscht werden. Zum einen werden Profile z. T. nur deaktiviert statt gelöscht. Zum anderen hinterlassen aktive Benutzer viele zusätzliche Informationen auf anderen Seiten des Netzwerkes. Diese allumfassend zu löschen, ist praktisch unmöglich. So verlieren Benutzerinnen und Benutzer die Kontrolle über ihre Daten.
- Bei den meisten SNS sind die Registrationshürden sehr niedrig: Man macht einige Angaben zur Person, die nicht getestet werden und also erfunden sein könnten. Dies ist zwar aus Datenschutzsicht positiv, weil die Person so unerkannt bleiben kann, birg aber auch Gefahren für diejenigen, welche mit solchen «erfundenen» Personen in Kontakt treten. Einmal drin, ist es unter Umständen sehr einfach, Kontakte zu schliessen und in die Freundeskreise anderer aufgenommen zu werden. Wenn Personen mit unlauteren Absichten sich als Freunde ausgeben und sich Informationen erschleichen, kann dies heikel werden.

Der typische Android-Nutzer (englisch):
http://allthingsd.com/20111229/if-android-were-a-single-person-heres-what-he-would-look-like/

2.1.2. Digitale Datensammlungen

Durch digitale Umfrage- und Wettbewerbsformulare, vor allem aber durch das «Web 2.0» mit seinen unzähligen Kommunikations-Plattformen und -Netzwerken, kommen Unmengen an Daten in Umlauf. Mit den heutigen Informationstechnologien ist es ein Leichtes, Personendaten zu erheben, zu speichern, zu analysieren, zu systematisieren und damit zu handeln. In der «web-community», der Internet-Gemeinschaft, kommt kaum jemand darum herum, dass seine Daten irgendwo Spuren hinterlassen und zu anderen Zwecken weiterverwendet werden.

In erster Linie geht es den Firmen auch hier um Werbeeinnahmen durch an den Benutzer angepasste Angebote. Den Risiken der modernen digitalen Technologien sind die folgenden Kapitel gewidmet.

2.1.3. Datenübertragung mittels digitaler Speichermedien

Von mobilen Datenspeichern, insbesondere von USB-Sticks gehen – oft unterschätzte – Gefahren aus. Sie können Viren übertragen und bei Verlust die Sicherheit von Personendaten gefährden. Befolgt man einige Regeln, lässt sich dieses Risiko allerdings stark verringern.

Laut Medienberichten sind in den letzten Monaten zahlreiche Organisationen über Speichermedien mit Schadenprogrammen infiziert worden. Einer amerikanischen Studie zufolge hat der Anteil der Virenübertragungen mittels USB-Sticks in den letzten Jahren stark zugenommen. Zur Übertragung der Viren reicht es aus, den Datenträger an den Computer anzuschliessen, und schon kann sich die «Malware» auf der Festplatte einnisten.

LanLine: Unterschätzte Schwachstelle USB-Stick
http://www.lanline.de/unterschaetzte-schwachstelle-usb-stick/

Dabei lassen sich die eigenen Daten relativ leicht vor Angriffen schützen, die von USB-Sticks ausgelöst werden.

- Die Autorun-Funktion für USB-Keys auf dem Computer sollte deaktiviert sein, um zu verhindern, dass Daten ungefragt übertragen werden. Dies lässt sich mit wenigen Klicks in der Systemsteuerung einrichten. Unter «Automatische Wiedergabe» kann das Häkchen auf «Nein» gesetzt werden, um zu verhindern, dass ein USB-Stick ungefragt gestartet wird.
- Zudem empfiehlt es sich, wie bei der Festplatte auch, den Stick regelmässig auf Viren zu überprüfen. Dazu sollte ein Reinigungsprogramm die Dateien auf dem Stick durchsuchen und gegebenenfalls bereinigen.
- Damit Personendaten im Fall eines Verlusts des Speichermediums nicht in falsche Hände geraten, sollten sie verschlüsselt werden.

Chip.de: UsbFix2017 (Virenscanner für USB-Sticks und Festplatten)
http://www.chip.de/downloads/UsbFix-2017_74217923.html

Selbstdatenschutz.info: Externe Festplatte verschlüsseln oder USB-Stick verschlüsseln mit Windows
https://www.selbstdatenschutz.info/windows/externe_datentraeger_verschluesseln/

2.1.4. Die digitale Datenflut birgt Gefahren

In den letzten beiden Jahrzehnten wurde unser Leben durch das World Wide Web und die damit verbundenen Dienstleistungen massiv verändert und – im positiven Fall – vereinfacht. Wir kommunizieren ohne Probleme und in Echtzeit rund um den Globus. Die dabei anfallende Datenmenge und der Datenaustausch verursachen aber auch Gefahren für die User. Persönliche Informationen, Texte, Filme und Fotos, die man ins Netz stellt, sind ab da nicht mehr privat. Einmal im Netz, entwickeln die Daten ein Eigenleben. Sie verbreiten sich, gelangen in Suchmaschinen und Online-Archive (z.B. thearchive.org), werden von anderen Nutzern kopiert und weitergereicht. Alles wieder rückgängig zu machen und zu löschen ist nahezu unmöglich.

Das World Wide Web vergisst (fast) nichts!

Viele Daten werden automatisch übertragen, ohne dass man es merkt.

Immer, wenn wir uns ins Internet begeben (egal ob zuhause am PC oder mit dem Smartphone), wird dies über eine sogenannte IP-Adresse (eine Art «Telefonnummer» im Internet) registriert. Damit lässt sich genau nachvollziehen, wann, wie lange und auf welchen Seiten unter dieser Nummer gesurft wurde. Die IP-Adresse wird zwar bei jedem Internetbesuch wieder neu zugeteilt, der Internetanbieter protokolliert aber alle Internetbesuche mit den IP-Adressen. Somit kann er jederzeit nachvollziehen, unter welche Nummer wie lange und wie oft gesurft wurde und welche Seiten dabei besucht wurden.

Über die IP-Adresse kann die Polizei bei Straftaten, zum Beispiel bei illegalen Musik-Uploads, den Täter ermitteln. Auch Unternehmen speichern IP-Adressen und können so unter Umständen feststellen, ob ein Rechner schon einmal auf die Webseite zugegriffen hat oder nicht. Man hinterlässt beim Surfen im Internet also einen **digitalen Fussabdruck**, der über unser Surfverhalten Auskunft gibt. Zudem hinterlässt das Surfen auch Spuren auf unserem Computer oder Smartphone.

2.2. Webtracking

2.2.1. Cookies

Mit Hilfe von sogenannten «**Cookies**» (*engl: Kekse*) werden Datenprofile erstellt. Die Profile beinhalten zum Beispiel Informationen über unsere Surfvorlieben, über die Bannerwerbung, die wir angeklickt haben, oder darüber, wie lange wir auf der jeweiligen Seite herumgesurft sind. Das Cookie selbst ist eine kleine Datei, die beim Lesen bestimmter Internetdateien vom Server auf die eigene Festplatte gespeichert wird. Dies kann praktisch sein, weil man beim Surfen und Besuchen von Angeboten im Web seine spezifischen Einstellungen (z.B. Sprache) nicht laufend neu eingeben muss, wird aber auch für andere Funktionalitäten gebraucht. Unangenehme Folgen sind aber nicht ausgeschlossen. Da Cookies unsichtbar abgespeichert werden, weiss der User in den meisten Fällen nicht, was es beinhaltet und auslöst: in vielen Fällen bedeutet dies eine unerwünschte verhaltens- und zielgruppenorientierte Werbeflut.

2.2.2. Einbindung von Social Plugins

Durch das Einbinden von Social Plugins können Webseitenbetreiber (Anbieter) gewisse Dienste von sozialen Netzwerken auf ihren eigenen Websites nutzen. Mithilfe des Like-Buttons von Facebook beispielsweise können die Seitenbesucher die Website mit einem Mausklick auf ihrem Facebook-Profil teilen. Die Anbieter erhoffen sich so eine schnelle Weiterverbreitung ihrer Seite. Daneben wird die Einbindung auch dazu genutzt, detaillierte Statistikinformationen über ihre Nutzer zu erhalten. Social Plugins lösen automatisch eine Datenübertragung an den jeweiligen Webseitenbetreiber aus. Bei Facebook beispielsweise werden bereits beim Seitenaufruf Daten wie die IP-Adresse des Seitenbesuchers und die Adresse der besuchten Seite übermittelt. Und das unabhängig davon, ob der Nutzer auf den «Like Button» geklickt hat, ob er bei Facebook eingeloggt oder überhaupt bei Facebook registriert ist. Ebenso wird, sofern vorhanden, ein bereits zu einem früheren Zeitpunkt angelegtes Cookie mit gesendet.

Ist der Internetnutzer beim Surfen gleichzeitig im sozialen Netzwerk eingeloggt, können die Trackingdaten direkt mit ihm in Verbindung gebracht werden. Klickt er auf den «Like Button», kommt die Information hinzu, dass ihm ein bestimmter Inhalt gefällt. So lassen sich detaillierte Nutzerprofile erstellen, mittels derer insbesondere personalisierte Werbung an die Nutzer und deren Freundeskreis im Netzwerk adressiert werden kann.

2.2.3. Was die Internetbenutzer gegen das Tracking tun können

Als Erstes empfiehlt es sich, **die gespeicherten Cookies und den Browserverlauf** nach jeder Sitzung zu löschen bzw. den Browser derart einzustellen, dass die Löschung automatisch bei jedem Schliessen des Programms erfolgt.
Der Nutzer hat zudem die Möglichkeit, die Speicherung von Drittanbieter-Cookies in seinem Browser zu sperren. Diese Strategie hilft allerdings nicht gegen sog. Flash-Cookies, die unabhängig vom Browser auf dem Rechner abgespeichert werden. Man sollte sie im **Einstellungs-Manager des Flash-Players** deaktivieren, der in der Systemsteuerung zu finden ist, sofern man diesen installiert hat.
Die Installation von kleinen **Software-Paketen («Add ons»)** im Browser erlauben es dem Nutzer zu beobachten, welche Tracking-Dienste ihn gerade verfolgen - und je nach Produkt lassen sich diese in den Einstellungen spezifisch sperren. Jedoch ist auch bei diesen kleinen Programmen Vorsicht geboten: vermeintlich nützliche Anwendungen können Trojaner enthalten, welche Dateien absaugen. Tipp: nur Apps aus vertrauenswürdigen Quellen herunterladen, regelmässige Updates durchführen und Apps löschen, die man nicht mehr braucht.
Viele Browser haben inzwischen eine sogenannte **Do-not-Track-Funktion.** Diese Option lässt sich im Browser einstellen und signalisiert, dass man nicht verfolgt werden möchte («do not track»).
Der Internetnutzer sieht allerdings nicht direkt, ob sich die Gegenseite daran hält. Aus datenschutzrechtlicher Sicht stellt die Nichtbeachtung einer solchen Widerspruchserklärung eine widerrechtliche Persönlichkeitsverletzung dar.

vgl. EDÖB, Erläuterungen zu Webtracking:
https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/webtracking/erlaeuterungen-zu-webtracking.html

Bluewin.ch – So erkennen Sie unsichere Websites
https://www.bluewin.ch/de/digital/redaktion/2017/17-07/so-erkennen-sie-unsichere-websites.html

2.3. Soziale Netzwerke und Chats

Beispiele: Facebook, Instagram, Snapchat, Twitter, Pinterest, etc.

Wer möglichst viele Funktionen Sozialen Netzwerken nutzen möchte, unterliegt rasch der Versuchung, möglichst viel Persönliches preiszugeben. Damit läuft man Gefahr, identifizierbar zu werden, und setzt sich diversen Risiken aus, beispielsweise der unerwünschten Kontaktaufnahme. Hier zeigt sich die Diskrepanz des sozialen Netzwerkens: «Ich muss mich zeigen, um dabei zu sein» - eine neue Form von sozialem Druck.

Inzwischen gibt es in allen «Social Networks» Einstellungsmöglichkeiten der Sichtbarkeit privater Informationen, die den Nutzer befähigen, selbst zu entscheiden, WIE sichtbar WELCHE Information für WEN sein soll.

Die untenstehende Grafik zeigt, welchen Stellenwert soziale Netzwerke in der Internetlandschaft heutzutage einnehmen.

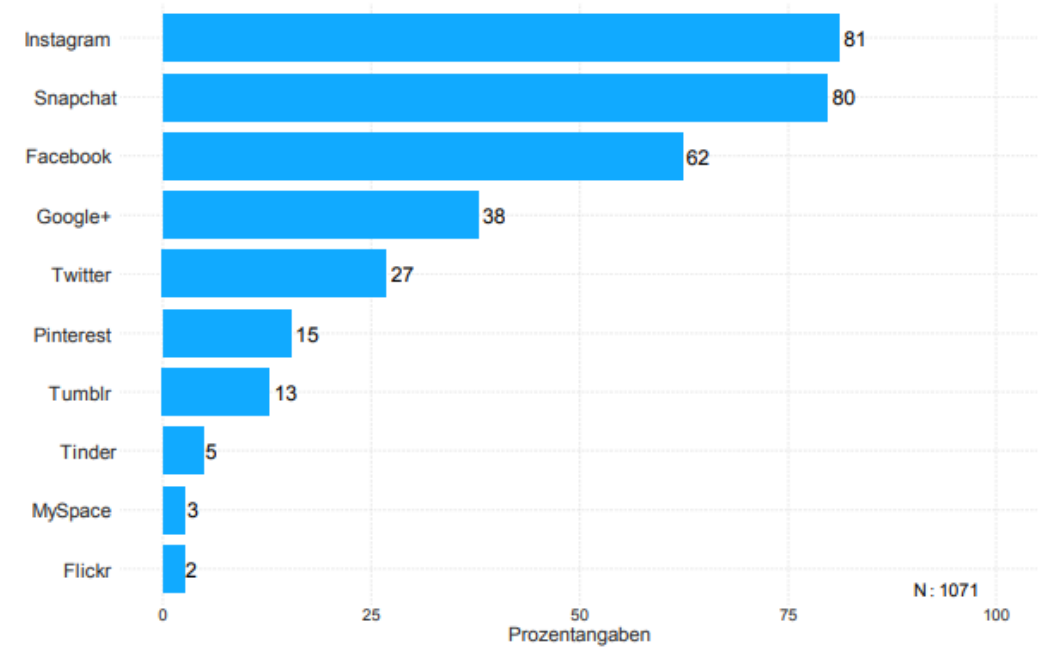

Abbildung 42: Mitgliedschaft bei Sozialen Netzwerken

(Quelle : https://www.zhaw.ch/storage/psychologie/upload/forschung/medienpsychologie/james/2016/Ergebnisbericht_JAMES_2016.pdf)

Problematisch ist, dass es immer Netzwerke gibt, bei denen die Sicherheitseinstellungen zum Schutz der Privatsphäre nach der Anmeldung im Netzwerk aktiv vorgenommen werden müssen. Wünschenswert wäre jedoch die Voreinstellung auf höchster Sicherheitsstufe bei der Anmeldung, die man auf eigenen Wunsch lockern kann («Privacy by default»).

Aber was, wenn eine technische Panne Fotos oder Kommentare preisgibt, die nur ein paar Freunde sehen sollten? Dass so etwas passieren kann, hat Visionär und Facebook-Gründer Mark Zuckerberg im Jahr 2011 am eigenen Leib erfahren: Einige seiner privaten Fotos waren kurzzeitig für alle Welt zu sehen – und sind nun an anderer Stelle im Netz zu finden.

Datenpanne legt Zuckerbergs Fotos frei
http://www.zeit.de/digital/datenschutz/2011-12/facebook-datenpanne?cid=1454131

2.3.1. Welche Daten sammelt Google?

Ende der 90er Jahre gründeten zwei Informatikstudenten das Unternehmen «Google». In erster Linie ist es für seine Suchmaschine bekannt. Inzwischen bietet Google aber auch zahlreiche andere populäre Onlinedienste an. Hier ein paar Beispiel von Daten, die wir Google wissentlich oder unwissentlich zur Verfügung stellen:

Google-Suche:
Länder-Code
Suchanfrage
IP-Adresse
Sprache
Anzahl der Ergebnisse
Safe search an/aus
Klicks auf Suchanfrage-Links
Cookies / Browsertyp

Youtube:
alle hochgeladenen Videos
alle Kommentare
Videos, die gemeldete wurden
Kanäle
angesehene Videos
Datentransfer
Klickverhalten
Land
Cookies / Browsertyp

Blogger:
Benutzerfotos
Geburtstag
Land
Datentransfer
Datengrösse
Klicks
Posts

Google-Konto:
Registrierungsdatum
Benutzername
Passwort
Alternative E-Mail-Adresse
Land
Anzahl der Logins
Genutzte Google-Dienste
Cookies / Browsertyp

Bei registrierten Usern:
E-Mail-Adresse
Passwort
Benutzername
Favoriten
Gruppen
Kontakte

Google-Docs:
E-Mail-Adresse
Anzahl der Logins
Anzahl der Aktionen
Datengrösse
Klicks
alle Texte
alle Bilder
alle Änderungen
Registrierungsdaten

Google Toolbar
Besuchte Webseiten (alle)
Alle 404-Seiten
Synchronisationsfunktion
mit dem Google-Account

Google Übersetzer
alle übersetzten Texte
Cookies / Browsertyp

Google Mail
Alle E-Mails
Alle Kontoaktivitäten
Speicherplatz
Anzahl Logins
angeklickte Links
Kontaktlisten
Datenverkehr
Datengrösse

Fazit:
Das sind nur einige der Dienste, die uns kostenlos angeboten werden. Wir sollten uns immer bewusst sein, dass diese Dienste nie wirklich «gratis» sind – wir bezahlen mit unseren Daten. Fakt ist, dass Google & Co sehr viele Daten sammeln. Das muss teilweise natürlich sein, weil sonst einige Dienste nicht funktionieren können. Wer aber sehr viele Dienste nutzt, der kann einsortiert und kategorisiert werden. Es können sehr weitreichende Persönlichkeitsprofile entstehen. In erster Linie werden solche Daten dafür verwendet, damit

Ihnen personalisierte Werbung zugestellt werden kann. Die Google-Suche optimiert anhand des Profils die Suchergebnisse. Der Suchende kommt so schneller an sein Suchergebnis, da er anhand eines Profils eingeordnet wird. Die Frage wird hier sein, ob ein User überhaupt will, dass er in eine Schublade gesteckt wird und ihm eine computergenerierte Selektion der Resultate präsentiert wird.

2.3.2. Warum sammelt z.B. Facebook-Userdaten?

Über die Kommunikationsplattform Facebook tauschen sich Menschen in aller Welt aus und sprechen nicht nur über Hobbies und Ansichten zur Entwicklung der Welt. Vielmehr nutzen viele Facebook auch als eine Art persönliches Gedächtnis oder Fotoarchiv, auf das sie weltweit zugreifen können. Nicht zuletzt für «mobile» Menschen bietet sich eine scheinbar günstige Möglichkeit, miteinander in Verbindung zu bleiben: Ein Internetzugang reicht. Wer verstehen will, warum Facebook - auch gelöschte – Daten der User sammelt, der sollte in die Historie des Unternehmens einsteigen und das Geschäftsmodell verstehen.

Werbeplattform Facebook

Die meisten Internet-Werbeangebote leiden darunter, dass sie beinahe ungezielt jedermann vorgeschlagen werden, der gerade auf eine Internetseite klickt. Die meiste im Internet als Banner oder Verlinkung geschaltete Werbung bleibt deshalb ungelesen, weil diese zu unspezifisch für den einzelnen User ist. Die Idee hinter dem sogenannten Sozialen Netzwerk Facebook ist es, Werbung zu personalisieren. Wenn man also Angaben zu seinem Beruf und seinen Hobbies macht, dann bekommt man entsprechende Werbung zugesendet. Entweder direkt auf der eigenen Profilseite oder bei Zustimmung zum Erhalt von Angeboten auf anderen Wegen auch per Mail oder via andere Kommunikationsplattformen. Damit vermeidet der Werbetreibende, dass er überflüssige Klicks bezahlt. Da sich jeder bei Facebook immer mit einem von ihm selbst gewählten Namen anmeldet, weiss das Unternehmen jederzeit, wer vor dem Rechner sitzt. Aus zusätzlichen Angaben wie Wohnort, Beruf und Alter kann auch das Einkommen geschätzt werden. Werbetreibende erfahren somit die Altersangabe, die Einkommensgruppe und je nach Angaben des Users auch die Interessen des Einzelnen.

Mit jedem Klick lernt Facebook den Nutzer näher kennen

Durch die beliebten «gefällt mir»-Buttons lernt Facebook jedes Mal etwas über seine Benutzer – also über uns und unsere Vorlieben. Wenn wir uns für Schiffsreisen begeistern, kann uns eine hochpreisige Luxuskreuzfahrt oder auch eine Clubkreuzfahrt für Junge angeboten werden. Deshalb sind praktisch alle Vergangenheitsdaten bares Geld wert. Mit jedem einzelnen Klick wird das Profil des Benutzers durchschaubarer und für die Werbeindustrie interessanter. Dies stellt den eigentlichen Wert von Facebook dar. Übrigens: Auch beim blossen «Ansurfen» einer Webseite mit Like-Button werden Daten an das Unternehmen geliefert und mit dem eingeloggten Profil verknüpft.

Durch zu viele Löschvorgänge wird Facebook wertlos

Eine von einem Wiener-Studenten ausgelöste Datenschutzuntersuchung bei Facebook rüttelt praktisch an den Grundfesten des Unternehmens. Wenn bisher angefallene Informationen einfach gelöscht werden können, erhält der Benutzer ein Stück weit die Kontrolle über sein Profil zurück. Facebook ist für die Werbeindustrie nur dann interessant, wenn vollständige

Informationen vorliegen. Die Firma hat nun selbst offenbart, dass der Bitte des Benutzers, Daten zu löschen, nicht nachgekommen wird. Diese werden in der Rechenzentrale nicht wirklich gelöscht, sondern deaktiviert, also auf einen «unsichtbaren» Status geschaltet.

Was kann der Facebook Benutzer dagegen tun?

Die konkrete Empfehlung lautet, eine persönliche Abwägung zu treffen. Jeder sollte für sich selbst entscheiden, wie viele Informationen er preisgibt und was er damit anstellen möchte. Wenn man ein selbstbestimmtes Leben führen möchte, dann sollte man Adressen, Bilder, Interessen, aber auch Meinungsäusserungen nur zurückhaltend im Internet preisgeben. Auf alle Fälle sollte man dort aber weder persönliche Daten hochladen, noch unbedarft Geschäfte abwickeln. In jedem Fall sollte man vorher die AGB und insbesondere die Datenschutzbestimmungen eines Onlinedienstes sorgfältig studieren.

Bitte beachten:

Jeder trifft eine persönliche Entscheidung: Was ist mir Freiheit wert und wie hoch wiegt der Vorteil einer bequemen, (beinahe) kostenfreien Nutzung? Und es gilt zu bedenken, mit welchen Informationen man auch in fünf Jahren noch konfrontiert werden möchte.
Denn das Internet vergisst bekanntlich nichts. Es liegt an jedem Einzelnen, selbst zu entscheiden.

2.3.3. Profil-Recherchen und –Fälschungen

Personen, mit denen Beziehungen jeglicher Art bestehen, insbesondere aktuelle oder künftige Arbeitgeber, können Personen «googlen» und Social-Network-Profile durchsuchen.
Nicht alles, was man über andere Menschen im Netz an Informationen findet, ist für diese vorteilhaft.
Profile können aber auch gefälscht sein, was für die Betroffenen sehr unangenehm sein kann. Den eigenen Namen mit auf SNS spezialisierten Suchmaschinen wie www.yasni.ch zu checken, kann solchen Missständen entgegenwirken. Die Betreiber der Websites mit den falschen Angaben sollte aufgefordert werden, die entsprechenden Seiten zu löschen bzw. die Angaben zu korrigieren.

2.3.4. Kriminelle Absichten

Die Daten des Profilinhabers können in die Hände von Personen mit unlauteren oder kriminellen Absichten geraten. Werden die Daten oder Informationen nicht genügend geschützt oder nicht sorgfältig mit ihnen umgegangen, können daraus unerwünschte Folgen resultieren.

2.3.5. Phishing

Phishing werden Versuche von Tätern genannt, an Daten eines Internet-Benutzers zu gelangen (z. B. Daten aus Profilen), damit Identitätsdiebstahl zu begehen und beispielsweise über gefälschte WWW-Adressen, E-Mails oder Kurznachrichten die entsprechende Person zu schädigen (z. B. Kontoplünderung).

Datenklau im Internet zwecks Aneignung einer fremden Identität kann gravierende Folgen - z. B. finanzieller oder rufschädigender Art – für das Opfer haben. Gerade in den Bereichen Online-Banking und Online-Handel, aber auch bei Single-Börsen ist Vorsicht geboten.

2.3.6. Online Shopping

Im Bereich Online-Shopping lauern viele Gefahren und Phishing kann gerade hier zum Problem werden. Heutzutage kann fast alles übers Internet gekauft werden und billige Angebote wecken das Interesse der Online-Kundschaft. Damit Online-Shopping nicht zum Frust wird, müssen Shops bei jedem Einkauf auf ihre Seriosität überprüft werden. Besonders bei Bestellungen im Ausland ist Vorsicht geboten. Fährt man bei bekannten Webseiten in der Regel gut, sollte man bei eher unbekannten die allgemeinen Geschäftsbedingungen unter die Lupe nehmen. Auch die Zahlungsmethode ist ein Indiz dafür, wie seriös ein Anbieter ist.

Tipps zum Schutz vor Betrug bei Online-Shopping und Auktionen – Schaugenau.ch
https://www.schaugenau.ch/de/betrug_und_datenklau#!betrug_bei_online-shopping_und_auktionen

Schutz vor Internet-Betrug – skppsc.ch
https://www.skppsc.ch/de/themen/internet/internet-cyberbetrug/

Einkaufen übers Internet – Wissen.de
http://www.wissen.de/einkaufen-uebers-internet

Phishing – Immer raffiniertere Betrugsversuche – Der Beobachter
https://www.beobachter.ch/konsum/konsumentenschutz/phishing-immer-raffiniertere-betrugsversuche

Geschichten aus dem Internet - Bundesamt für Kommunikation (BAKOM)
http://www.thewebsters.ch/de/

Vorsicht Internetfallen (Broschüre) – Staatssekretariat für Wirtschaft (SECO)
https://www.seco.admin.ch/seco/de/home/Publikationen_Dienstleistungen/Publikationen_und_Formulare/Werbe_und_Geschaeftsmethoden/Unlauterer_Wettweberb/vorsicht-vor-internetfallen-.html

2.4. Konkrete Gefahren und rechtliche Folgen

2.4.1. Cyber-Stalking

Von Cyber-Stalking ist die Rede, wenn die elektronischen Kontaktmöglichkeiten der SNS böswillig dazu benutzt werden, jemanden zu bedrängen. Ausserdem kann die Menge an Daten, die die Benutzerinnen und Benutzer über sich selbst bekanntgeben, durchaus dazu führen, dass jemand die Wohnadresse seines Opfers herausfindet, seine Lebensgewohnheiten kennenlernt und es so physisch verfolgen kann.

Stadtpolizei Zürich, Schaugenau.ch – Cyberstalking (Tipps und Handlungsmöglichkeiten)
https://www.schaugenau.ch/de/belaestigungen#!cyber-stalking

2.4.2. Cyber-Mobbing

Wird eine Person über das Internet von anderen über längere Zeit belästigt, schikaniert oder regelrecht terrorisiert – was unter Kindern und Jugendlichen immer wieder vorkommt-, nennt man das auch Cyber-Mobbing. Dabei wird das Opfer mit verfälschten, peinlichen oder offenherzigen Bildern oder Videos oder mit beleidigenden Informationen, die im Internet

publiziert werden, belästigt. Auch über gefälschte Profile in Online-Communities (z. B. Instagram, Facebook) können Täter ihre Opfer plagen und in Schwierigkeiten bringen. Opfer solcher Attacken leiden stark unter den Angriffen.

Was sagt das Recht über Cyber-Mobbing?

- Werden Videos oder Bilder ohne Zustimmung veröffentlicht, wird damit die Privatsphäre und das Recht am eigenen Bild verletzt.
- Wer per E-Mail, Instant Messenger, SMS oder andere Kanäle Mitmenschen fortlaufend beleidigt oder belästigt, kann sich strafbar machen.
- Werden, beispielsweise in Foren, Sozialen Netzwerken oder Blogs, Unwahrheiten verbreitet oder Beleidigungen ausgesprochen, kann man Unterlassungsanspruch geltend machen oder Strafanzeige erstatten. Belästigung, Drohung, üble Nachrede, Verleumdung, Erpressung, Nötigung etc. gelten als Straftatbestände, egal durch welches Medium, egal ob öffentlich oder geschlossen. **Solche Vorfälle sollten der Polizei gemeldet werden.**

2.4.3. Cyber-Bullying

Man versteht darunter das wiederholte und willentliche Tyrannisieren von Personen durch Veröffentlichung von Beleidigungen, Erniedrigungen oder Androhung von Gewalt im Internet. Das Wort «Bullying» bedeutet etwa tyrannisieren, schikanieren oder gar terrorisieren.

We live security – Cyber Mobbing vorbeugen
https://www.welivesecurity.com/deutsch/2017/02/07/safer-internet-day-2017-cyber-mobbing-vorbeugen/
Blick.ch – Schwyzer Schüler stellen Lehrer mit Hass-Profilen bloss.
https://www.blick.ch/news/schweiz/fotomontage-mit-ku-klux-klan-schwyzer-schueler-stellen-lehrer-mit-hass-profilen-bloss-id7663188.html

2.4.4. Sexting und Sextortion

«Sexting ist die private Kommunikation über sexuelle Themen per mobile Messaging. Im engeren Sinn handelt es sich um Dirty Talk zur gegenseitigen Erregung. Seit Verfügbarkeit der Multimedia Messaging Services (MMS) und Instant-Messagern wie WhatsApp kann damit auch der Versand von erotischem Bildmaterial des eigenen Körpers über Instant-Messaging-Anwendungen durch mobile Endgeräte verbunden sein.»
Definition: Wikipedia https://de.wikipedia.org/wiki/Sexting

Obwohl die private Kommunikation auch über sexuelle Themen grundsätzlich strafrechtlich erlaubt ist, gibt es datenschutzrechtliche und strafrechtliche Risiken zu beachten:

- Wer Bilder oder Filme von sich verbreitet, macht sich strafbar, wenn das sexuelle Gewalttätigkeiten oder Handlungen mit Tieren sind. Das ist illegale Pornographie.
- Darstellungen von Sex unter Minderjährigen (unter 18-jährige) oder sexy Darstellungen Minderjähriger gelten als Kinderpornographie und haben strafrechtliche Konsequenzen. Unter 18-jährige sollten darüber unbedingt Bescheid wissen.

- Als Kinderpornographie gelten einerseits Darstellungen sexueller Handlungen mit Minderjährigen (unter 18). Verboten sind auch sexualisierte Darstellungen von Minderjährigen – auch wenn dabei keine sexuellen Handlungen gezeigt werden –, also z. B. auch Selfies Minderjähriger in einer eindeutig sexy Pose. Es ist verboten, Kinderpornos herzustellen, zu schauen, zu besitzen oder zu verschicken. Sexting kann Kinderpornographie sein!

(Quelle: https://www.lilli.ch/sexting_kinderpornografie/)

Website Illegale Pornografie – skppsc.ch
https://www.skppsc.ch/de/themen/sexuelle-uebergriffe/illegale-pornografie-pornosucht/

Informationsbroschüre Pornografie: Alles was Recht ist – skppsc.ch
https://www.skppsc.ch/de/wp-content/uploads/sites/2/2016/12/rechtpornografie.pdf

- Das grösste Risiko bei Sexting besteht darin, dass die Inhalte sehr schnell verbreitet werden, sich aber nur schwer löschen lassen. Mit einem einzigen Klick landet ein kompromittierendes Bild oder Video im Internet und bleibt womöglich für immer. Auch wenn die Bilder bewusst geschickt werden – etwa an eine vertrauenswürdige Person, oder unter Gruppendruck – können sie schlimme Probleme verursachen, wenn sie in die falschen Hände und/oder an eine breite Öffentlichkeit gelangen.
- Bei «Sextorsion» handelt es sich um eine Form der Erpressung im Zusammenhang mit Sexting. Ein Erwachsener beschafft sich unter einer falschen Identität über soziale Netzwerke oder über das Internet freizügige Bilder von Jugendlichen und droht, sie zu veröffentlichen, um noch mehr Bilder (z.B. Striptease vor laufender Webcam), Geld oder ein Treffen mit dem Opfer zu erzwingen.

(Quelle: http://www.jugendundmedien.ch/chancen-und-gefahren/gefahren-im-ueberblick/sexting.html)

Fazit:
Wie schon vorgängig öfters erwähnt, gilt auch hier das Prinzip: Das Internet vergisst nie! Es muss also wohl überlegt sein, ob die verschickten Bilder oder Videos für jedermann bestimmt sind, da eine Veröffentlichung, sei sie gewollt oder ungewollt, nie ausgeschlossen werden kann. Was einmal im Internet ist, kann jederzeit wieder auftauchen. Hilfe und Beratung findet man in solchen Fällen bei Pro Juventute (Tel. oder SMS an 147 oder unter 147.ch), einer kantonalen Opferberatungsstelle oder auch bei Schulsozialarbeitern, Lehrpersonen und selbstverständlich bei den Eltern oder anderen engen Bezugspersonen (Familie und gute Freunde). Wichtig ist, dass die Vorfälle angesprochen und aufgedeckt werden, so dass Massnahmen ergriffen werden können, dass das veröffentlichte Material aus dem Internet entfernt werden kann und weitere Übergriffe vermieden werden können.

Link zu den Adresslisten der Opferberatungsstellen
http://www.sodk.ch/fachbereiche/familie-und-gesellschaft/opferhilfe/wwwopferhilfe-schweizch/adresslisten/

2.5. Smartphones

Heute verfügt ein Smartphone über unzählige Zusatzprogramme. Einige dieser Anwendungen / Apps kann man zunächst kostenfrei verwenden und dann durch eine Kauf-Funktion aufstocken oder Werbefreiheit herstellen. Bei manchen Apps entstehen regelmässige Abo-Kosten. Apps sammeln Daten der Nutzer, die das in der Regel weder erfahren noch steuern können. Erfasst werden zum Beispiel Ort, Zeit und Häufigkeit von Programmnutzungen sowie SMS und gespeicherte Kontaktdaten. So gönnen sich z. B. Instagram und Facebook einen vollständigen Zugriff auf die Gerätedaten inklusive Standort und SMS.

2.5.1. Geolokalisierung – Fluch oder Segen?

Bei der Geolokalisierung wird einer IP-Nummer oder sonstigen Identifikations-Adressen die geografische Position zugeordnet. Eine andere Möglichkeit den Standort eines Users zu ermitteln, ist der Zugriff über GPS oder WLAN. Was bei Computern in vielen Fällen Sinn und einige Apps – Programme und Anwendungen – überhaupt erst nützlich machen kann (z. B. Navigations-Apps), muss bei der Lokalisierung von Smartphones kritisch beurteilt werden.

Andere darüber informieren, wo man sich gerade aufhält, ist heute angesagt. Dahinter lauern aber auch Gefahren. Wir geben damit zum Beispiel preis, ob wir gerade zuhause sind, was auch für Einbrecher interessant sein kann.

Aber auch sonst gilt es sich zu fragen, ob alle Welt jederzeit wissen soll und muss, wo sich ein User gerade aufhält. Die grösste Gefahr bei der Nutzung der Standortfunktion bei Onlinediensten und Apps liegt darin, dass die Lokalisierungstechnik auch dazu verwendet werden kann, Bewegungsprofile anzulegen. Selbst wenn diese nicht in jedem Fall einer Person zuzuordnen sind, sind die gesammelten Daten vieler Internet- und Smartphone-Nutzer ein interessantes Mittel zur Marktforschung und der Industrie eine Menge Geld wert.

Google Maps Timeline, Google speichert Ihr Bewegungsprofil, so löschen Sie es:
http://www.chip.de/news/Google-Maps-Timeline-Google-speichert-Ihr-Bewegungsprofil-so-loeschen-Sie-es_81310080.html

2.5.2. Strafrecht

Bestimmte Inhalte sind generell verboten und strafbar: dazu gehören **ehrverletzende, rassistische, kinderpornografische und jugendgefährdende Inhalte**. Es kann auch strafbar sein, im Internet Links auf Seiten mit solchen Inhalten zu setzen oder solche «heiklen» Inhalte von Handy zu Handy weiterzugeben. Wichtig: Die Weitergabe von Pornos an unter 16-Jährige ist verboten!

2.6. Videotelefonie

Beispiele: Skype, FaceTime, Google Hangouts, Viber

Die Videotelefonie hat in den vergangenen Jahren eine immer bedeutendere Rolle in der Kommunikation weltweit erlangt. Sowohl geschäftlich als auch privat tauschen sich viele Personen nicht mehr nur verbal und schriftlich, sondern auch unterstützt durch Bild- und Tonübertragung aus. Verschiedene Anbieter sind auf diesen Zug aufgesprungen und haben ihre Kommunikationsangebote mit der Option zur Videotelefonie ausgerüstet.

Bei der Auswahl des Messenger gilt es aber Verschiedenes im Auge zu behalten:

- Sind die Inhalte auf dem Verkehrsweg verschlüsselt?
- Sind sie vor den Einblicken der Anbieter sicher, indem die Schlüssel auf den Geräten der Nutzer und nicht den Servern gespeichert sind?
- Sind ältere Nachrichten unter Umständen nachträglich einsehbar, wenn sie bloss durch kurzlebige Schlüssel (Passwörter, die nach einer gewissen Zeit ablaufen) geschützt sind?

(Quelle: http://www.zeit.de/digital/datenschutz/2014-11/messenger-sicher-vergleich-eff)

Nebst dem Anbieter ist auch der Gesprächspartner kritisch zu betrachten. Chats mit unbekannten Personen sind insofern kritisch, als Bild und Ton eventuell mitgeschnitten und aufgenommen werden könnten, ohne dass die betroffene Person dies merkt. Heikle Daten, persönliche Aussagen und kompromittierendes Bildmaterial sollten deshalb nicht per Videochat verschickt, bzw. gezeigt werden.

Skype: Anonyme Chats gefährden die Privatsphäre
http://www.onlinewarnungen.de/warnungsticker/skype-anonyme-chats-gefaehrden-die-privatsphaere/

2.7. Bilder und Bildrechte

2.7.1. Noch schnell etwas online stellen …? (Recht am eigenen Bild)

Wenn mit dem Smartphone, Handy oder einem anderen Gerät Fotos oder Filme aufgenommen werden und diese durch unüberlegten Upload schnell ins Internet gelangen, wird sehr rasch das **Recht am eigenen Bild** verletzt, wenn auf den Aufnahmen Personen erkennbar sind.

Unabhängig von urheberrechtlichen Überlegungen besteht bei Fotos das Recht am eigenen Bild. Dies bedeutet, dass die abgebildeten Personen in der Regel darüber entscheiden, ob und in welcher Form ein Bild aufgenommen und veröffentlicht werden darf. Aus diesem Grund dürfen Fotos meist nur dann veröffentlicht werden, wenn die darauf Abgebildeten ihr Einverständnis gegeben haben.

Eine Einwilligung ist – nur dann – nicht nötig,

- wenn die abgelichteten Personen nur als Beiwerk neben einer Landschaft oder einer sonstigen Örtlichkeit erscheinen.
- nicht die teilnehmenden Personen im Vordergrund stehen.
- wenn die Bilder Personen der Zeitgeschichte (also auch Prominente) zeigen.

Also aufgepasst bei Partys, Konzerten und Discobesuchen: Nicht jedes Foto, nicht jeder Film, darf ungefragt online gestellt werden!

Zudem ist es sicher ratsam, auch etwas kritisch zu sein, was die Veröffentlichung der eigenen Bilder angeht: schnell wird «in der Hitze des Gefechts» eingewilligt, dass ein mitunter vielleicht etwas heikles Bild auf einem Klatschportal oder in einem Social Network landet. Auch mit Selfies sollte man sorgfältig umgehen.

Übrigens hat nur der Fotograf das Recht zur Veröffentlichung. Ein Foto zu veröffentlichen, ohne den Urheber vorher um Erlaubnis gefragt zu haben, ist nicht erlaubt – egal, wie oft das Foto bereits im Internet verfügbar ist.

2.7.2. Gruppenfotos

Auch bei Gruppenfotos können die Persönlichkeitsrechte der betroffenen Personen tangiert sein, sobald diese auf dem Foto erkennbar sind. Der Eingriff in die Persönlichkeitsrechte wiegt dann weniger schwer, wenn keine Einzelperson aus der Gruppe heraustritt und als solche wahrgenommen wird.

2.7.3. Aufnahmen im öffentlichen Raum

Werden Fotos im öffentlichen Raum aufgenommen, ist dies für alle Anwesenden erkennbar und sind die Abgebildeten nur «Beiwerk» (z.B. Passanten bei einer Sehenswürdigkeit), so ist es ausreichend, wenn das entsprechende Bild auf Verlangen der fotografierten Personen (sofort vor Ort sowie zu jedem späteren Zeitpunkt) gelöscht bzw. auf eine Veröffentlichung verzichtet wird. Die betroffenen Personen müssen jedoch nicht zusätzlich angesprochen und informiert werden.

2.7.4. Die rechtsgültige Einwilligung

In allen anderen Fällen muss die Einwilligung der Betroffenen eingeholt werden. Sie ist immer nur dann gültig, wenn sie nach angemessener Information und freiwillig erfolgt. Widerspricht eine betroffene Person der Veröffentlichung, ist dies zu respektieren.

Wer Bilder einzelner Personen aufnimmt und veröffentlicht, muss anders vorgehen. Hier ist die oben beschriebene generelle Einwilligung nicht ausreichend. Vielmehr müssen die Betroffenen die Möglichkeit haben, die zur Publikation vorgesehenen Bilder einzusehen und sich über den Kontext der Veröffentlichung zu informieren. Zudem gilt es zu beachten, dass bei der Publikation von Bildern Minderjähriger auch die Zustimmung der erziehungsberechtigten Personen eingeholt werden muss.

2.7.5. Mögliche Konsequenzen bei Veröffentlichungen ohne Rechtfertigungsgrund

Personen, deren Bilder ohne Rechtfertigung veröffentlicht wurden, können sich jederzeit gegen die Veröffentlichung wehren und ihre Ansprüche nötigenfalls mittels Zivilklage geltend machen. Kommt das Gericht zum Schluss, dass eine widerrechtliche Persönlichkeitsverletzung vorliegt, weil die Fotos ohne Einwilligung oder überwiegendes öffentliches bzw. privates Interesse veröffentlicht wurden, so kann es nebst der Entfernung bzw. Vernichtung der fraglichen Bilder auch die Bezahlung von Schadenersatz und/oder einer Genugtuung anordnen.

(Quelle: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/veroeffentlichung-von-fotos.html)

2.8. Andere Technologien

2.8.1. Datenübermittlung in eine Cloud

Beispiele: iCloud, One Drive, Dropbox

Das Auslagern von Daten in eine sogenannte «Cloud« (engl. Wolke) bringt für den Benutzer den Vorteil, dass nicht der lokale Speicherplatz auf dem PC, Laptop oder auch auf dem Smartphone gefüllt wird, sondern die Daten online gespeichert werden. Viele Apps nutzen diese Speichermöglichkeit automatisch und laden Inhalte des Handybenutzers in eine Cloud, teilweise auch, ohne dass der Nutzer es merkt. So werden bei einigen Foto-Anwendungen (z. B. Google Fotos) die Bilder nach der Aufnahme direkt in einer Cloud gespeichert, sofern dies durch den Benutzer nicht deaktiviert wird.

Risiken bei der Nutzung von Clouds:

- **Kontrollverlust über die Daten:** Wegen der weltweiten Vernetzung und der Virtualität ist der Standort der Daten oft nicht erkennbar. Dies trifft im besonderen Mass für die Public Clouds zu. Der Cloud-Nutzer weiss damit nicht, wo genau seine Daten in der Cloud gespeichert und verarbeitet werden. Er weiss oft auch nicht, ob Subunternehmer involviert sind und ob diese für einen angemessenen Datenschutz sorgen.

- **Zugriff von ausländischen Behörden auf die Daten:** In vielen Fällen werden die Daten für die Bearbeitung in der Cloud ins Ausland bekannt gegeben. Dabei werden die Daten oftmals auch in Ländern gespeichert oder bearbeitet, die über keinen (ausreichenden) Datenschutz verfügen. Cloud-Service-Anbieter sind aber auch gegenüber ausländischen Behörden und Gerichten verpflichtet, gegebenenfalls Zugriff auf Daten in der Cloud zu gewähren; dies gilt selbst dann, wenn die Daten nicht im Land der Behörde bearbeitet oder gespeichert werden.

Die nachfolgenden Risiken bestehen immer, unabhängig davon, ob die Datenbearbeitung in einer Cloud stattfindet oder nicht.

- **Datenverlust:** Daten können durch Diebstahl, Löschung, fehlerhafte Überschreibung oder sonstige Veränderung verloren gehen.

- **System- und Netzwerkausfälle** sowie Nichtverfügbarkeit angemieteter Ressourcen und Services können dazu führen, dass Daten verloren gehen oder unberechtigten Personen zugänglich werden und dass damit die Vertraulichkeit, Sicherheit und Integrität der Daten nicht mehr gewährleistet ist.

Fazit:

Der Cloud-Nutzer sollte sich gut überlegen, welche Anwendungen und Daten er bei sich behalten will und welche in die Cloud wandern sollen.
(Quelle: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/cloud-computing/erlaeuterungen-zu-cloud-computing.html)

2.9. «Internet der Dinge»

Das Internet der Dinge bezeichnet die Vernetzung von Gegenständen mit dem Internet, damit diese Gegenstände selbstständig über das Internet kommunizieren und so verschiedene Aufgaben für den Besitzer erledigen können. Der Anwendungsbereich erstreckt sich dabei von einer allg. Informationsversorgung über automatische Bestellungen bis hin zu Warn- und Notfallfunktionen.

(Quelle: http://wirtschaftslexikon.gabler.de/Archiv/1057741/internet-der-dinge-v4.html)

Beispiele: Fitnessarmbänder, vernetzte Haushaltgeräte (z. B. Thermostat, Stromzähler, Smart TV, Drucker, Spielzeuge mit Mikrofon und/oder Kamera).

(Quelle: Pixabay / Pixabay)

Viele der elektronischen Geräte und Features, welche durch ihre Vernetzung zum Internet der Dinge gezählt werden, sind kleine Helfer im Alltag. Auch wenn sie auf den ersten Blick das Leben erleichtern und gewisse Aufgaben sogar selbständig ausführen können, gilt es auch hier skeptisch zu sein.
Damit unser Leben nicht durch diese Geräte bestimmt wird, müssen wir sicher sein, dass sie uns nicht nur gehören, sondern auch gehorchen. Das ist nicht immer einfach.
Wenn diese Geräte mit dem Internet verbunden sind, sind sie häufig nicht ausreichend geschützt.
Einige Funktionen sind sogar Absicht: Fernseher petzen den Sendern, was wir wann schauen oder hören gar mit, Lautsprecher zeichnen unsere Wohnzimmergespräche auf.
Wenn Sie sich ein vernetztes Dingsda kaufen wollen, sollten Sie – schon bevor Sie sich über Produkt-Features und Herstellerauswahl Gedanken machen – Folgendes überlegen:

1. Brauche ich das Gerät wirklich oder erfüllt es nur denselben Zweck wie ein anderes Gerät, das ich schon habe (bzw. mir einfach ausleihen kann), sieht aber einfach besser aus? Ist gar der Hauptzweck des Geräts nur anzugeben, cool zu scheinen oder dazugehören zu wollen?
2. Brauche ich die vernetzten Funktionen wirklich? Auch wenn das bedeutet, dass ein Bösewicht das Gerät möglicherweise vollständig fernsteuern kann? Stellen Sie sich dabei das Schlimmste vor und gehen Sie davon aus, dass der Bösewicht noch einmal um einiges einfallsreicher ist als Sie. Sind die Zusatzfunktionen den Aufpreis und das erhöhte Risiko wert?
3. Falls die vernetzte Funktion jemals aussteigt (der Hersteller stellt seinen Cloud-Dienst ein) oder deaktiviert werden muss (Sicherheitsbedenken): Kann ich das Gerät dann noch weiternutzen?

(Quelle: http://www.pctipp.ch/tipps-tricks/kummerkasten/sicherheit/artikel/weg-vom-internet-der-unsicheren-dinge-87430/)

«Internet der Dinge – Datenschützer moniert fehlende Transparenz», NZZ Online
https://www.nzz.ch/schweiz/aktuelle-themen/internet-der-dinge-datenschuetzer-moniert-fehlende-transparenz-ld.116181

Tipps für den richtigen Umgang mit Daten

2.10. Grundsätze

Sorgfältiger Umgang mit Daten und Informationen:

- Nur so viele persönliche Daten preisgeben wie für den Zweck nötig.
- Bei Formularen (Wettbewerbe etc.) und Online-Profilen persönliche Angaben sparsam verwenden. Daten sparen!
- Wenn möglich keine Angaben über Adresse, Telefonnummer, Alter (v.a. bei Kindern) machen.

Respekt: die goldene Regel (ein Grundsatz aus der praktischen Ethik)

- «Andere so behandeln, wie man selber behandelt werden möchte.»
- «Was du nicht willst, dass man dir tu`, das füg` auch keinem anderen zu.»

2.11. Konkrete Tipps

2.11.1. Allgemeine Sicherheitstipps

- Verwendung von **sicheren Passwörter** – mindestens 8-stellig, Kombination aus Gross- und Kleinbuchstaben, Ziffern und Sonderzeichen und sichere Aufbewahrung gewährleisten.
- Bei jedem Dienst ein anderes Passwort verwenden (es gibt nützliche Passwortmanager wie z. B. KeePass, weil man sich nicht so viele verschiedene sichere Passwörter merken kann).
- Sichere Konfiguration des Internet-Browser, d.h. mit privatsphärefreundlichen Einstellungen.
- Regelmässiges Löschen von Cookies.
- Löschen des Browser-Verlaufes, insbesondere an öffentlichen Computern.
- Verwendung einer Antivirensoftware und regelmässige Aktualisierung.
- Software von vertrauenswürdigen Anbietern/Quellen verwenden (insbesondere bei Add-ons) – Vorsicht bei Gratis-Programmen.
- Verwendung von **aktueller Software** resp. regelmässige Updates machen
- Verwendung von Verschlüsselungstechniken beim Übermitteln von Daten. (auf grünes Sperrschloss in der Adressleiste achten. Dieses signalisiert eine verschlüsselte Verbindung.)

2.11.2. Soziale Netzwerke

Beispiele: Facebook, Instagram, Google+, Youtube

- Jeder ist für den Schutz seiner Privatsphäre selbst verantwortlich!
- Darauf achten, wie man sich im Netz zeigt.
- Merke: Alles, was wir schreiben, posten, verlinken etc. gibt auch Auskunft über uns.

- Peinliche Fotos, Filme und sehr persönliche Informationen haben nichts im Netz zu suchen. Sie verraten viel Persönliches, können den Ausbildungsplatz kosten oder Ärger verursachen.
- Überlegen, was eine Gruppenmitgliedschaft über einen aussagt.
- Sorgfältig sein mit Profil-Daten: Adresse, Telefonnummer, E-Mail-Adresse etc. besser weglassen.
- Profileinstellungen auf privat setzen. Nur Freunde sollen die Angaben sehen.
- Überprüfen, ob «Online-Freunde» wirklich gut genug bekannt sind, um ihnen freien Zugang zu privaten Fotos und Daten zu geben. Man kann nicht wissen, was sie mit den Informationen machen!
- Beiträge erst nach gründlicher Überprüfung bzw. Überlegung posten.
- (Allzu) Negative Emotionen und Stellungnahmen vermeiden. Oft schreibt man im Affekt Dinge, die man später bereut.
- Bilder, Adressen und andere Daten (auch Markierungen auf Fotos) von Freunden, Bekannten etc. nur mit deren Einwilligung hochladen.
- Kurz: Die richtige Auswahl an Informationen treffen, die man verbreiten will.
- Die Privatsphäre-Einstellungen regelmässig überprüfen und diese gegebenenfalls anpassen.

2.11.3. Smartphone und WLAN

- WLAN-Netzwerke nur verschlüsselt betreiben. Zugang mit Passwort schützen, Vorsicht bei der Weitergabe des Passwortes. Besser: Gastnetzwerke einrichten.
- Das WLAN abschalten, wenn es nicht in Gebrauch ist. Das erhöht die Sicherheit, weil es Angriffe auf die Funkschnittstellen verhindert -, und spart Akku.
- Bei öffentlichen Hotspots und WLAN-Angeboten vorsichtig und kritisch sein (auf E-Banking verzichten und Zurückhaltung bei Login auf Internetdienste wie soziale Netzwerke).
- Heikle und wichtige Daten wenn möglich, nur verschlüsselt nutzen und verschicken.
- Die GPS-Ortung nur gezielt d.h. bei effektivem Bedarf aktivieren (bei Freigabe stets überlegen, ob die Ortung für einen Dienst / eine App notwendig ist).
- Apps nur aus sicheren Quellen beziehen (offizielle App-Stores).
- Vor dem Download einer App, sollte man sich mittels Beschreibung und Bewertungen über den Nutzen und den Inhalt informieren und die ABG und Datenschutzbestimmungen lesen.
- Sicherheitseinstellungen der Betriebssysteme nutzen: Die aktuellste Betriebssoftware nutzen, indem man Updates sofort installiert.
- Den Zugriff der Apps auf notwendige Informationen beschränken. Ist es notwendig, dass die App z. B. auf Kontakte, Kalender, GPS und Nachrichten zugreifen kann?

Verlust des Smartphones – Nicht nur das Gerät ist weg, auch persönliche Daten sind in Gefahr!

- Zumindest den Zugriff durch Fremde kann man durch die vorsorgliche Eingabe eines Passwortes bei Inbetriebnahme und Entsperrung erschweren oder sogar verhindern.
- Manche Unternehmen bieten eine Software zum «Fernlöschen» der Daten vom heimischen PC aus an.
- Regelmässiges Backup erstellen und verschlüsseln (lokal, statt in der Cloud).

2.11.4. Digitale Speichermedien

- Deaktivieren der Autorun-Funktion für USB-Sticks auf dem Computer.
- Standardmässige Überprüfung des Datenträgers auf Viren.
- Ausschliessliche Verwendung von Speichermedien aus sicheren Quellen und von Personen, denen man vertrauen kann.

Verlust des USB-Sticks oder der portablen Festplatte – die Daten sind in Gefahr!

- Verschlüsselung von sensiblen und heiklen Personendaten auf digitalen Speichermedien!

2.11.5. Chats

- Chats auswählen, in denen jemand aufpasst (Moderator).
- Einen guten Nickname ausdenken (Fantasienamen, lustige Wörter, einen Namen, der keine heiklen Assoziationen weckt). Nicht den richtigen Namen, keine Altersangabe, den Wohnort oder die Schule.
- Adresse, Telefonnummer oder Nachnamen sollten nie verraten werden.
- Respektvoller Umgang und richtiger Ton: es gilt die «Chatiquette» (siehe unten).
- Vorsicht beim persönlichen Treffen mit Leuten aus dem Chat (Eltern Bescheid sagen).
- Ein gesundes Misstrauen hilft. Nicht zu viel Persönliches preisgeben.
- Nicht direkt mit Fremden «flüstern».

Wenn einem etwas komisch vorkommt:

- Sofort reagieren und Bescheid sagen! Helfen können Eltern, eine Vertrauensperson oder Lehrpersonen.
- Den Dialog umgehend beenden.

Chatiquette - Der gute Ton im Netz: http://www.chatiquette.de/

2.11.6. Foren und Blogs

Beispiele: Twitter (Mikroblogs), Blogger (Google), Webforen (unzählige)

Netiquette

Die erste und grundlegende Empfehlung der Usenet-Netiquette ist:
«Vergiss niemals, dass auf der anderen Seite ein Mensch sitzt!»
(Quelle: http://www.usenet-abc.de/wiki/Team/Netiquette)

Allgemeine Netiquette-Kodizes:

- Verzicht auf Beleidigungen, Höflichkeit geht vor.
- Man fasst sich so kurz wie möglich.
- Ironische Äusserungen sollten vermieden werden.
- Korrekte Schreibweise (inkl. Gross- und Kleinschreibung).
- Korrektes Zitieren (inkl. Anführungs- und Schlusszeichen, wenn nötig, bzw. wenn möglich mit Quellenangabe).
- Erst nach gründlicher Überprüfung der Inhalte posten.

2.11.7. Online-Formulare von Firmen, Dienstleistern und Behörden

- Grundsatz: Persönliche Daten nur an verlässliche Kontakte weitergeben und nur dann, wenn man einen Nutzen davon hat.
- Die AGB – die Allgemeinen Geschäftsbedingungen – insbesondere den Abschnitt «Datenschutz» genau lesen. Hier erfährt man, welche Personendaten gespeichert, weitergegeben oder für Werbung genutzt werden. Und sich dann genau überlegen, ob man eine App unter den gegebenen Bedingungen tatsächlich verwenden möchte.
- Bei allen Bezahldiensten (Kreditkarten, Paypal etc.) ist besondere Vorsicht geboten: Kritisch sein!
- Niemals Auskunft über Benutzerdaten, Kreditkartennummern und Passwörter geben. Banken kontaktieren ihre Kunden nicht per E-Mail und fragen schon gar nicht nach einem Passwort oder dem Benutzernamen.
- In verdächtigen E-Mails keine Anhänge oder Links öffnen.
- Informationen über den Anbieter einholen und dessen Seriosität prüfen.
- Überprüfen, was man bei Phishing-Attacken tun kann.

Wie verhalte ich mich richtig bei Phishing?
https://www.skppsc.ch/de/themen/internet/phishing/
https://www.schaugenau.ch/de/betrug_und_datenklau#!phishing
https://www.melani.admin.ch/melani/de/home/themen/phishing.html

2.11.8. Instant Messenger und Internet-Telefonie

Beispiele: Skype, WhatsApp, Snapchat etc.

Allgemeine Sicherheitstipps:

- Auswahl eines Messenger, der Sicherheitseinstellungen zulässt.
- Den Messenger so einstellen, dass neue Kontakte akzeptiert werden müssen, bevor sie in die Kontaktliste aufgenommen werden.
- Die eigene Messengerkennung (Ihren Benutzernamen) nicht leichtfertig an fremde Personen weitergeben.
- Nur wirklich gute Freunde in die Kontaktliste aufnehmen und nur diesen erlauben, selbst auf deren Liste gesetzt zu werden (bei einigen Messenger lässt sich dies nicht mehr rückgängig machen).
- Löschen von unliebsamen, unanständigen und aufdringlichen Kontakten oder diese mit der «Ignore-Funktion» sperren.
- Nur Nachrichten / Anrufe von Personen in der eigenen Kontaktliste annehmen.
- Die öffentliche Statusanzeige ausschalten.
- Den Nachrichtenverlauf automatisch speichern.
- Das Anzeigebild und die Webcam-Übertragung ausschalten.
- Grundsätzlich keine Dateien oder Links von unbekannten Personen öffnen. Diese können Viren, Trojaner etc. enthalten. Ebenso wie die Video- oder Telefonübertragung lässt sich dies leider nicht bei allen Messenger automatisch blockieren.
- Keinesfalls auf einen erhaltenen Link im Nachrichtenfenster klicken, ohne sich vorher abgesichert zu haben, dass die jeweilige Person diesen auch tatsächlich willentlich geschickt hat. Wie bei E-Mail-Würmern können sich eingefangene Schädlinge selbständig an die Personen aus den Kontaktlisten verschicken. Auch wenn Links von

Bekannten kommen, können sich dahinter also Gefahren verbergen und der Sender weiss selbst nichts davon.

2.12. Daten anderer: Sei fair!

- Die Persönlichkeitsrechte anderer müssen beachtet werden!
- Keine Bilder, Filme und Informationen (z. B. Benutzernamen, Nummern, Adressen, Passwörter etc.) von anderen ohne deren Erlaubnis ins Netz stellen!
- Auf **sensible Daten** achten!
- Es ist unbedingt zu vermeiden, Neuigkeiten über andere zu verbreiten, die die betroffenen Personen selbst nicht veröffentlichen wollen oder noch nicht selbst veröffentlich haben.
- Es ist verboten, falsche oder herabmindernde Informationen über jemanden zu veröffentlichen. Rufschädigung kann bestraft werden!

Strafrecht beachten

- Ehrverletzende, volksverhetzende, (kinder-) pornografische und jugendgefährdende Inhalte dürfen nicht weitergegeben und verbreitet werden.
- Im Zweifelsfall heisst es: Die Finger davon lassen und eine Vertrauensperson informieren!

Schweizerisches Strafgesetzbuch (StGB):

u.a. Art. 19714. Pornografie

4. Pornografie

1 Wer pornografische Schriften, Ton- oder Bildaufnahmen, Abbildungen, andere Gegenstände solcher Art oder pornografische Vorführungen einer Person unter 16 Jahren anbietet, zeigt, überlässt, zugänglich macht oder durch Radio oder Fernsehen verbreitet, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

(Quelle: https://www.admin.ch/opc/de/classified-compilation/19370083/index.html)

Sich selbst bleiben!

Das Internet ist nur scheinbar ein anonymer Raum und schon gar kein rechtsfreier.
Man sollte also nicht machen, was man im wirklichen Leben nicht auch tun würde.
Es gilt alles zu vermeiden, was man später bereuen könnte.
Sauber bleiben, sich selbst bleiben. Auch im Netz!

3. Glossar

3.1. Begriffe zum Datenschutz

Gläserner Mensch	Vollständige Durchleuchtung des Menschen und seines Verhaltens. Bezug zum Datenschutz: Durch die Preisgabe persönlicher Informationen riskieren wir den Verlust unserer Privatsphäre.
Informationelles Selbstbestimmungsrecht	Jeder Mensch soll selbst darüber bestimmen können, welche Informationen über ihn wann, wo und wem bekannt gegeben und zu welchem Zweck sie verwendet werden dürfen.
Personenbezogene Daten (od. Personendaten)	Angaben über eine bestimme oder eine bestimmbare Person. Es genügt also, wenn man aus den Daten darauf schliessen kann, zu wem sie gehören. Es muss nicht zwingend ein Name genannt werden.
Besonders schützenswerte Daten	Besonders heikle Informationen und Daten, bei denen besondere Sorgfalt gefordert ist. Dazu gehören beispielsweise religiöse oder politische Aktivitäten, Informationen, welche die Intimsphäre betreffen und Daten zur Gesundheit.
Privatsphäre	Nichtöffentlicher Bereich, in welchem ein Mensch unbehelligt von äusseren Einflüssen sein Recht auf freie Entfaltung der Persönlichkeit wahrnehmen kann.
Intimsphäre	Bereich der innersten bzw. persönlichsten Gedanken und Gefühle eines Menschen. Bereich des Erlebens, über den eine Person üblicherweise nicht gerne spricht und den sie der Umwelt gegenüber aus Takt oder Bewahrung des Selbstgefühls sorgfältig abschirmt (z.B. Sexualität)

3.2. Begriffe aus dem Bundesgesetz über den Datenschutz

Bearbeiten	Jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren; insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten.
Bekanntgeben	Das Zugänglichmachen von Personendaten wie das Einsicht gewähren, Weitergeben oder Veröffentlichen.
Betroffene Personen	Natürliche (Private) oder juristische Personen (Firmen), deren Daten *bearbeitet* werden.
Datensammlung	Jeder Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach betroffenen Personen erschliessbar sind (z. B. über Suchfunktionen).

Inhaber der Datensammlung	Private Personen oder Bundesorgane, die über den Zweck und den Inhalt der Datensammlung entscheiden und dafür verantwortlich sind.

3.3. Begriffe rund ums Internet

Banner	Werbefläche (im Internet mit Verlinkung zu einer Domain / einer Website)
Browser	Software, mit der Inhalte aus dem WWW dargestellt werden. Computerprogramm, um ins Internet zu gelangen (z. B. Internet Explorer, Google Chrome, Firefox)
Chat	Möglichkeit der Echtzeit-Kommunikation mehrerer Teilnehmer über das Internet. Onlinekommunikation, die über die Tastatur ausgeführt wird. Der User kann zwischen einzelnen «Chatrooms» wählen und auch entscheiden, mit wem er (nicht) «reden» möchte.
Cookies	Textdateien, die beim Aufruf von Internetseiten beim Benutzer generierte werden. Darin werden Informationen über das Nutzungsverhalten des Users festgehalten. Cookies können von aussen abgefragt werden. Sie lassen sich in den Browsereinstellungen aber auch sperren.
Domain	Alphanumerische Aliase für IP-Nummern / -Adressen. Domains können thematisch oder geographisch gegliedert sein. *Beispiele:* *.com = kommerzieller Anbieter* *.ch = Schweizer Anbieter, bzw. in der Schweiz registrierter Domain-Name* *.org = ursprünglich nicht-kommerzielle Domain* *.edu = Schulen und Universitäten*
Firewall	Ein Zwischenrechner, der ein Netzwerk vom Internet trennt. Er dient dem Schutz gegen Viren und vor unberechtigten Zugriffen auf das eigene Netzwerk.
FTP	File Transfer Protocol. Ermöglicht den Austausch von Dateien zwischen zwei Computern, die mit dem Internet verbunden sind (und beide das Protokoll FTP aktiviert haben). So können Dateien auf einen Internet-Rechner kopiert werden oder von diesem geladen werden.
Hacker	Person, die sich unbefugt Zugriff zu fremden Computersystemen verschafft.
http	Das Hypertext Transfer Protocol (http) ist ein Protokoll zu Übertragung von Daten über ein Netzwerk. Es wird hauptsächlich eingesetzt, um Webseiten aus dem World Wide Web (WWW) in einen Webbrowser zu laden.

https	Auch SSL HTTPS. Eine Methode, um Daten verschlüsselt zu übertragen. Dabei werden die Dateien mit SSL verschlüsselt und über das http übertragen.
IP-Adresse	Eine Art «Telefonnummer» für eine Internet-Session. Sie setzt sich aus vier Zahlenblöcken zwischen 0 und 255 zusammen, die mit einem Punkt voneinander getrennt sind. *Beispiel: 62.2.169.0*
Malware	Bösartige Software – Schadprogramme (manchmal synonym mit Viren verwendet), die vom User unbeabsichtigt oder unbemerkt installiert werden und auf dem Computer Schaden anrichten.
Newsgroup	Diskussionsforum in Internet.
Social Media	Siehe Web 2.0
SNS	Social Network Services – Anbieter von Sozialen Netzwerken *Beispiel: Facebook*
SSL	Verschlüsselungstechnik für das Internet.
Provider	Anbieter von Internetdienstleistungen. *Beispiele: upc, swisscom, sunrise*
URL	Uniform Ressource Locator. Ein System, das es ermöglicht, ein Angebot im Internet zu erreichen. Könnte auch als die «Adresse» eines Web-Angebotes bezeichnet werden. *Beispiel: www.sbb.ch*
***Web* 2.0**	Interaktive Anwendung im Internet. Der User ist nicht nur Konsument, sondern wird durch das Einbringen und Hochladen von Informationen und Daten selber aktiv.
WLAN	Wireless Local Area Network – drahtloses Netzwerk.

Internet-Lexikon für Eltern und Kinder

https://www.internet-abc.de/eltern/lexikon/ (Eltern / Erwachsene)
https://www.internet-abc.de/kinder/lexikon/ (Kinder)

4. Quellen, Links und Verweise

Thema / Stichworte	Link
Eidgenössischer Datenschutz-Beauftragter	www.derbeauftragte.ch/
Datenschutz im Internet	https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer.html
Tipps und Informationen zu Internet	http://www.jugendundmedien.ch/home.html http://netla.ch/de https://www.datak.ch http://www.klicksafe.de/
Sicherheit im Internet	https://www.skppsc.ch/de/ http://www.schaugenau.ch/de/home
Gewalt und Gefahren im Internet	http://www.jugendundmedien.ch/chancen-und-gefahren/gefahren-im-ueberblick/gewalt.html http://www.netcity.org/
Chat-Tipps	http://medienundschule.ch/fit4chat/ http://www.kinder-im-internet.ch/themen/vorbereitung-wissen/fit4chat/
Soziale Netzwerke	http://www.jugendundmedien.ch/chancen-und-gefahren/soziale-netzwerke.html
WLAN	https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/wlan.html
Cloud Computing	https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/cloud-computing/erlaeuterungen-zu-cloud-computing.html
Handy	https://www.handysektor.de/
Link-Sammlung (Jugendliche / Internet)	https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/jugend-und-internet/links-zum-thema.html
Informationen für Eltern	http://www.projuventute-elternberatung.ch/ https://www.internet-abc.de/

5. Verzeichnis von Ansprechpartner für verschiedene Probleme

5.1. Datenschutz

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
Kontaktformular:
https://www.edoeb.admin.ch/edoeb/de/home/der-edoeb/kontakt/kontaktformular.html
oder Tel. +41 (0)58 462 43 95

5.2. Für Eltern und Lehrpersonen

Elternnotruf: 0848 354 555 oder elternnotruf.ch

Übersicht der regionalen Beratungsstellen:
http://www.jugendundmedien.ch/de/beratung-und-angebote/beratungsangebote.html

LCH – Dachverband Lehrerinnen und Lehrer Schweiz
https://www.lch.ch/publikationen/bildung-schweiz/

5.3. Für Kinder und Jugendliche

Beratung und Hilfe von Pro Juventute:
Telefon und SMS 147, Informationen und Fragen-Antworten auf 147.ch

Websites für Jugendliche (Information, Fragen-Antworten, Foren):
feel-ok.ch, tschau.ch, cybersmart.ch, frageinfach.ch, lilli.ch und drgay.ch

Adressen der kantonalen Opferhilfe-Beratungsstellen (OHG) für Kinder und Jugendliche:
http://www.sodk.ch/fileadmin/user_upload/Fachbereiche/Opferhilfe/Adresslisten/2018.06.06_OH-Beratungsstellen_Kinder_und_Jugend.pdf

Netla - Kampagne des Rats für Persönlichkeitsschutz
http://www.netla.ch/de

6. Online-Artikel und Dossiers

Nr.	Thema / Stichworte	Link
1	Datenschutz, Internet, Zukunft	https://www.tagesanzeiger.ch/digital/internet/Der-Datenschutz-hat-nicht-die-staerkste-Lobby-in-der-Schweiz/story/11059030
2	Datenschutz, Internet, E-Mail	http://www.spiegel.de/netzwelt/web/ropemaker-sicherheitsluecke-macht-e-mails-angreifbar-a-1164373.html
3	Datenschutz, Software, Gesichtserkennung	https://www.tagesanzeiger.ch/digital/daten/Wir-verlieren-unser-Gesicht/story/29341015
4	Datenschutz, Internet, Kinder, Surfverhalten	https://www.tagesanzeiger.ch/digital/internet/Keine-Kontrolle-ueber-surfende-Kinder/story/10950714
5	Internet, Kinder und Jugendliche, Surfverhalten	https://www.mpfs.de/studien/jim-studie/2016/
6	Facebook-Dossier (20 Minuten)	http://www.20min.ch/digital/dossier/facebook/
7	Facebook, Datenschutz	http://www.luzernerzeitung.ch/nachrichten/digital/Facebook-soll-beim-Datenschutz-einlenken;art308,129143
8	Facebook, Datenschutz, Gesetz	https://www.blick.ch/news/schweiz/social-media-bundesrat-will-gesetzesluecken-zu-facebook-twitter-und-co-stopfen-id2471164.html
9	Facebook, Telefonnummern	https://www.tagesanzeiger.ch/digital/mobil/warum-facebook-die-telefonnummern-der-whatsappnutzer-will/story/26123699
10	Facebook, Privatsphäre	http://www.sueddeutsche.de/digital/smartphonekolumne-diese-privatsphaere-einstellungen-bei-facebook-sollten-sie-kennen-1.3004230
11	Facebook, falsche Freunde	https://www.tagesanzeiger.ch/zuerich/verbrechen-und-unfaelle/auf-facebook-sind-falsche-freunde-aktiv/story/10875168
12	Facebook, eigene Dateien	https://irights.info/artikel/inhalte-auf-facebook-veroffentlichen-was-muss-ich-beachten/11555
13	Fahndung via Facebook	https://www.welt.de/vermischtes/article121759470/Polizei-zwischen-Fahndung-und-Lynchsystem.html
14	Google-Dossier (20 Minuten)	http://www.20min.ch/digital/dossier/google/
15	Cloud Computing	https://www.netrics.ch/cloud-computing-schweiz-datenschutz/
16	Youtube-Film hochladen: Anzeige?	https://www.welt.de/regionales/hamburg/article159513125/Umstrittene-Youtuber-kassieren-Strafanzeigen.html
17	Smartphones, Apps, Personendaten	https://www.beobachter.ch/konsum/multimedia/datenschutz-im-internet-so-schutzen-sie-ihre-daten-vor-google-co
18	IPhone, Apple, Personendaten	https://www.blick.ch/news/schweiz/datenschutz-datenschuetzer-kritisieren-apple-id1417269.html
19	Smartphone, Android, Personendaten	http://www.20min.ch/digital/webpage/story/18588753
20	Personendaten, Laptop-Diebstahl	https://www.tagesanzeiger.ch/digital/computer/Schweizer-droht-LaptopDieb-mit-Pranger/story/24932714
21	Phishing	https://www.melani.admin.ch/melani/de/home/themen/phishing.html

7. Der EDÖB in den Medien

Link zu einer Auswahl von Interviews und Artikeln zu aktuellen Themen im Bereich Datenschutz: https://www.edoeb.admin.ch/edoeb/de/home/aktuell/medien/der-edoeb-in-den-medien.html