educa.Guides

Datenschutz
Sicherer Umgang mit Personendaten

Schule und ICT

Impressum

Herausgeber educa.ch

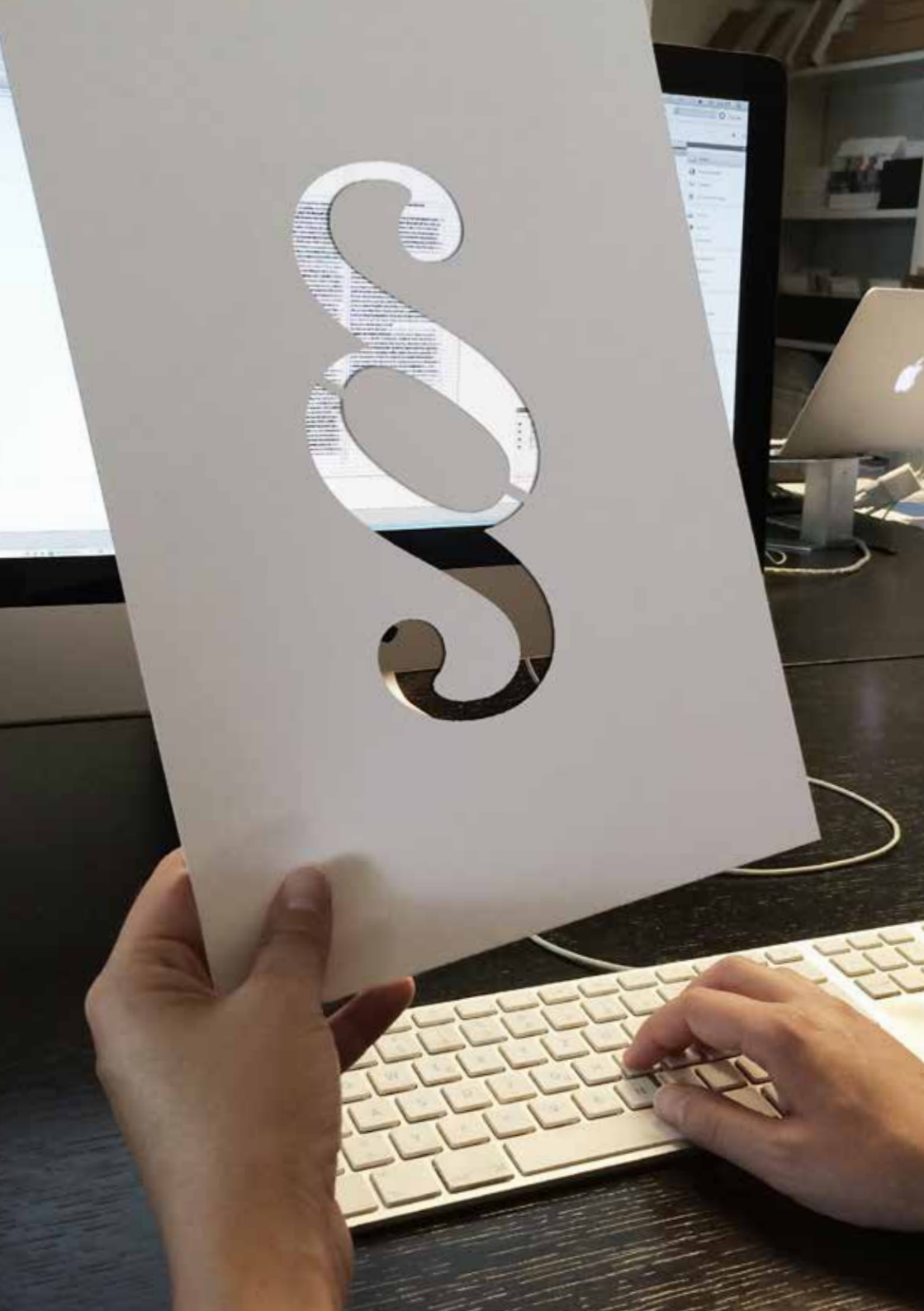
Auszüge mit freundlicher Genehmigung aus folgenden Quellen:
- Erziehungsdirektion Bern:
  Leitfaden zum Datenschutz in den Volksschulen des Kantons Bern (Nachschlagewerk)
- Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB):
  Datenschutz, Erläuterungen zu Sozialen Netzwerken, Einige Sicherheitshinweise zu WLAN

Fotos büro z {grafik design}, Bern

November 2009

Dieser Guide verfügt über eine Internetseite auf educa.ch. Hier finden Sie sowohl das vorliegende PDF, das Sie dort auch online einsehen können, wie auch Zusatzinformationen und Links auf Unterrichtsmaterial, die regelmässig aktualisiert werden. Das PDF ist mit dem Datum seiner Publikation und einer eventuellen Aktualisierung versehen und gibt den Informationsstand dieses Datums wieder.

→ Internetseite



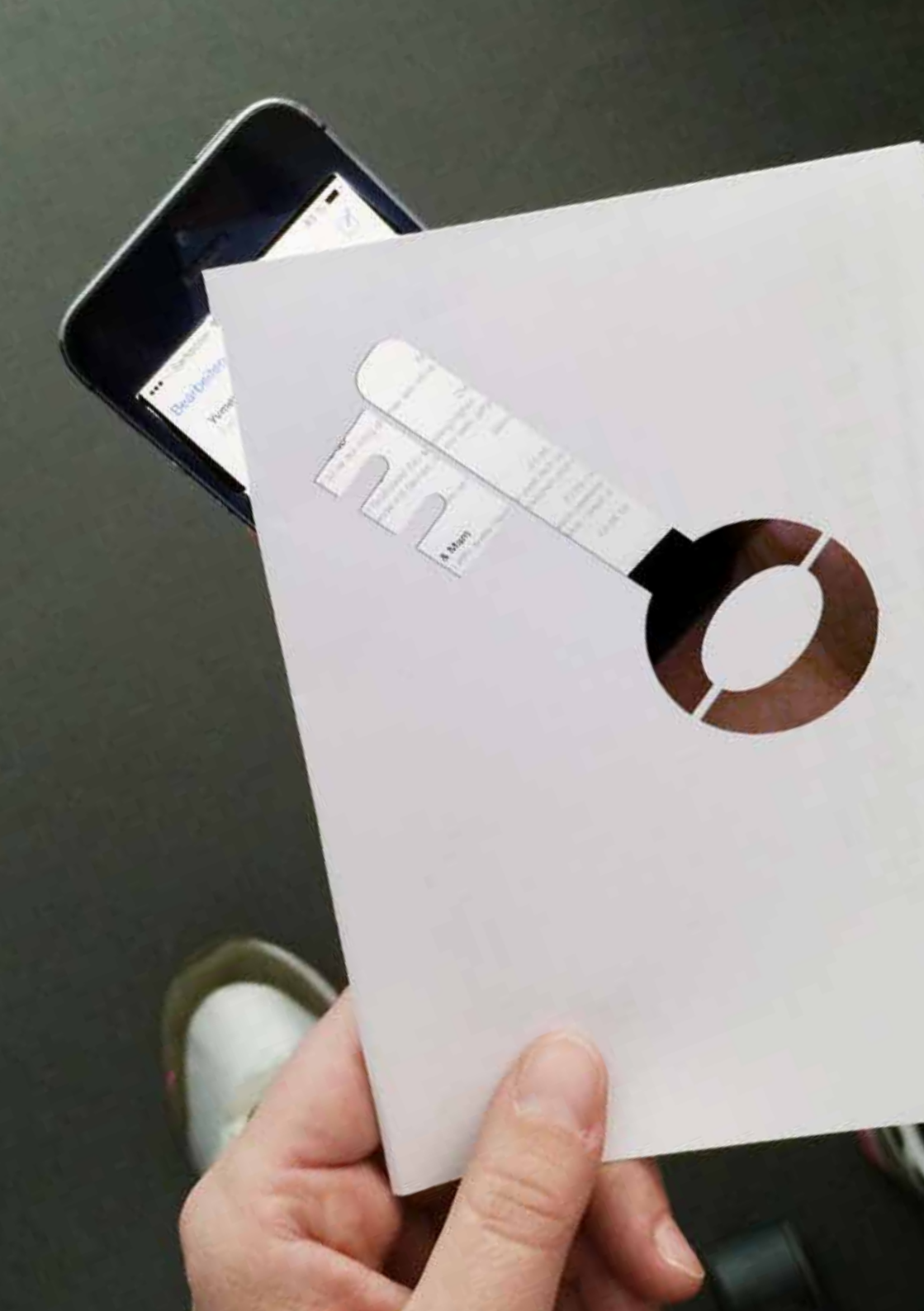
Einleitung

«Datenschutz» heisst nicht in erster Linie Schutz von Daten an sich, wie das Wort fälschlicherweise vermuten lässt, sondern Schutz der Menschen vor jedem Missbrauch ihrer persönlichen Daten in ihrem täglichen Leben. Spätestens seit Web 2.0 Applikationen Einzug ins Schulzimmer gehalten haben, kommt dem Schutz der persönlichen Daten von Lernenden – aber auch von Lehrenden - eine immer grössere Bedeutung zu. Leider sind sich viele Lehrpersonen der Brisanz der Datenschutzthematik noch zu wenig bewusst, denn in der Zeit vor der Einführung von Web 2.0 Diensten mussten sich vor allem die Schulverwaltungen und die Erziehungsbehörden mit dem Thema befassen, etwa wenn es darum ging, persönliche Daten von Schülerinnen und Schülern von einer Amtsstelle an eine andere weiter zu leiten. Inzwischen betrifft das Thema Datenschutz alle in der Schule Tätigen, denn kaum jemand wird heute ganz darauf verzichten wollen, interaktive Internetdienste zu nutzen.

Europäischer Datenschutztag

Der Europäische Datenschutztag, initiiert vom Europarat, wird jedes Jahr am 28. Januar begangen und soll den europäischen Bürgerinnen und Bürgern ermöglichen, zu verstehen, welche Daten über sie gesammelt und bearbeitet werden, zu welchem Zweck und welche Rechte sie dabei haben. Er ist auch eine Gelegenheit, sie für die Risiken zu sensibilisieren, die mit der illegalen Nutzung oder Verarbeitung ihrer persönlichen Daten verbunden sind.

→ coe.int



Grundsätzliches zum Datenschutz

Das erste Kapitel enthält eine Einführung zum Thema Datenschutz. Dabei werden folgende Fragestellungen aufgegriffen: Welche Daten müssen geschützt werden? Welche gesetzlichen Grundlagen zum Datenschutz existieren?

Informationelles Selbstbestimmungsrecht
Das so genannte informationelle Selbstbestimmungsrecht bildet einen wichtigen Grundsatz unserer gesellschaftlichen Ordnung. Informationelle Selbstbestimmung bedeutet, dass jeder Mensch so weit wie nur möglich selber darüber bestimmen können soll, welche Informationen über ihn wann, wo und wem bekannt gegeben werden.

Wozu dient Datenschutz?

Vereinfacht ausgedrückt könnte man sagen: Das erste Ziel des Datenschutzes muss sein, das informationelle Selbstbestimmungsrecht der Person zu verteidigen.

Diese Aufgabe ist nicht immer einfach, da es zum Teil auch legitime Interessen geben kann, die dieses Selbstbestimmungsrecht einschränken, so etwa bei polizeilichen Ermittlungen.

Verhältnismässigkeit

Der Datenschutz soll grundsätzlich gewährleisten, dass in jedem einzelnen Fall von Datenbearbeitung immer die Verhältnismässigkeit gewahrt bleibt, d. h. dass in keinem Fall mehr persönliche Daten gesammelt werden, als für die Erfüllung einer bestimmten, d. h. örtlich und zeitlich begrenzten Aufgabe unbedingt nötig ist. Und dass man als betroffene Person auch die Möglichkeit hat, die Bearbeitung der Daten über sich so weit wie möglich zu kontrollieren und notfalls zu verhindern.

Einsichtsrecht

Daher ist es unabdingbar, dass jeder über die Möglichkeit verfügt, von den Inhaberinnen und Inhabern von Datensammlungen Rechenschaft darüber zu erhalten, welche Daten über die eigene Person bearbeitet werden. Zu diesem Zweck schreibt das Datenschutzgesetz ein Einsichtsrecht über die eigenen persönlichen Daten vor, das bei den Inhaberinnen und Inhabern von Datensammlungen geltend gemacht werden kann.

Wie und wo ist der Datenschutz im Gesetz definiert?

Art. 13 der Bundesverfassung legt grundlegend fest, dass jede Person Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs sowie auf Schutz vor Missbrauch ihrer persönlichen Daten hat.

Der Datenschutz schützt somit nicht Daten an sich, sondern die Grundrechte von Personen.

Bundesgesetz über den Datenschutz

Um diesen Schutz gesetzlich zu verankern, wurde das Bundesgesetz über den Datenschutz (DSG) verabschiedet, das seit dem 1. Juli 1993 in Kraft ist. Die entsprechende Verordnung (VDSG) regelt die Einzelheiten.

Das Bundesgesetz über den Datenschutz (DSG) richtet sich an die Bundesverwaltung sowie an alle privaten Personen, die Personendaten bearbeiten.

Kantonale Datenschutzgesetze

Ausserdem existieren auch in anderen Gesetzen zahlreiche Bestimmungen zum Schutz der Persönlichkeit. In den Artikeln 28 – 28l des Zivilgesetzbuches z. B. wird festgelegt, wie im Fall von Persönlichkeitsverletzungen rechtlich vorgegangen wird.

Die kantonalen Datenschutzgesetze regeln die Datenbearbeitung durch kantonale Verwaltungen und sie bilden die Grundlage für die Datenschutzreglemente der Gemeinden. Diese wiederum sind rechtliche Grundlage für die von den Gemeinden geführten Schulen.

Welche Daten werden durch das Gesetz geschützt?

Personendaten sind Angaben über eine bestimmte Person. Unter Angaben ist jede Art von Information zu verstehen. Darunter fallen Tatsachenfeststellungen und Werturteile, ungeachtet der verwendeten Technik (analoges oder digitales Zeichen, Wort, Bild, Ton oder eine Kombination derselben) und ungeachtet der Übermittlungsart (unter Anwesenden, per Post oder elektronische Übermittlung). Nicht erfasst ist dagegen das Wissen einer Person, welches nirgends festgehalten oder gespeichert ist. Wird der Name und alle weiteren Elemente, welche eine Zuordnung zu einer bestimmten Person erlauben würden, entfernt, handelt es sich nicht mehr um Personendaten.

Bearbeitung von Personendaten
Unter den Begriff der «Bearbeitung» fällt jeder Umgang mit Personendaten, namentlich Beschaffung, Aufbewahrung, Veränderung, Verknüpfung, Bekanntgabe oder Vernichtung.

Bekanntgabe von Personendaten
Unter der «Bekanntgabe» von Personendaten versteht man jedes Zugänglichmachen von Personendaten, namentlich Einsichtgewährung, Auskunftgeben, Weitergabe oder Veröffentlichung.

Besonders schützenswerte Personendaten
Sobald es um «besonders schützenswerte» Personendaten geht, ist besondere Vorsicht geboten.
«Besonders schützenswerte» Personendaten sind:
- Angaben über die religiöse, weltanschauliche oder politische Ansicht, Zugehörigkeit und Betätigung
- Angaben über den persönlichen Geheimbereich, insbesondere über den seelischen, geistigen oder körperlichen Zustand
- Angaben über die Sozialhilfebedürftigkeit oder Abhängigkeit von fürsorgerischer Betreuung
- Angaben zu laufenden polizeilichen Ermittlungen, Strafverfahren, etc.

Bild- und Tonaufnahmen
… gehören nicht grundsätzlich zu den «besonders schützenswerten» Personendaten. Besonders schützenswert sind sie nur, wenn sie eine der oben erwähnten Angaben enthalten (wenn also beispielsweise die Symptome von Krankheiten auf Bildern erkennbar sind oder wenn aufgrund eines Bildes auf eine Religionszugehörigkeit geschlossen werden kann).

Obwohl Bild- und Tonaufnahmen nicht per se zu den «besonders schützenswerten» Personendaten gehören, bedeutet das nicht, dass im Umgang mit Bild- und Tonaufnahmen, welche nur «normale» Personendaten enthalten, nicht auch sehr vorsichtig umgegangen werden muss. Nicht zuletzt die Veröffentlichung von Personenbildern auf dem Internet kann schwerwiegende und kaum abschätzbare Auswirkungen auf die Persönlichkeitsrechte der betroffenen Personen haben, z. B. durch den Missbrauch der Bilder auf anderen Websites, durch Verunglimpfung der abgebildeten Personen mit Hilfe von Bildbearbeitungsprogrammen, etc.


AF-L
AF-L
OK

Schutz von Daten im Unterricht mit ICT

Dieses Kapitel richtet sich in erster Linie an Lehrpersonen und Lernende. Es zeigt insbesondere die verschiedenen Gefahren auf, welche mit der Benutzung von interaktiven Internetdiensten – sog. Web 2.0 Applikationen – einher gehen. Am Schluss des Kapitels folgt eine Liste mit Empfehlungen zum Umgang mit Web 2.0 Applikationen, welche sich an alle in der Schule Tätigen richtet.

Mangelndes Sicherheitsbewusstsein

Die Informationstechnologie ermöglicht es, enorme Mengen von Personendaten zu erfassen und diese miteinander in Verbindung zu setzen. Leider hält das Sicherheitsbewusstsein der Datenbearbeitenden oft nicht mit den technischen Neuerungen Schritt. Zudem sind die meisten Menschen – seien es die Bearbeitenden von Daten oder die Personen, deren Daten bearbeitet werden – noch nicht genügend für Fragen des Persönlichkeitsschutzes sensibilisiert. Nur allzu leichtfertig geht man mit seinen persönlichen Daten um, ob im Internet oder beim Ausfüllen von Umfrage- oder Wettbewerbsformularen, um nur zwei Beispiele zu nennen.

Surfen, Soziale Netzwerke, Chat

Benutzerinnen und Benutzer des Internets sind zunehmend nicht mehr nur «Konsumenten», die von Providern zur Verfügung gestellte Informationen auf statischen Websites suchen und downloaden, sondern benutzen das Internet interaktiv und arbeiten an dynamischen Websites mit. Diese Entwicklung wird unter dem Begriff Web 2.0 zusammengefasst.

In diesem Zusammenhang sind verschiedene Social Networking Sites (SNS) entstanden. Es sind dies umfangreiche Portale, in denen sich angemeldete Benutzerinnen und Benutzer treffen, sog. «Freundschaften» schliessen und Nachrichten, Fotos und Filme austauschen.

SNS stellen den Datenschutz vor neue Herausforderungen. Datenschutzgesetze waren ursprünglich darauf ausgerichtet, Personendaten vor der unrechtmässigen oder übermässigen Bearbeitung durch den Staat, später auch durch kommerzielle Unternehmen zu schützen. Mit den SNS sind nun zwei grundlegend neue Aspekte aufgetaucht:

– Die genannten persönlichen Informationen werden von den Benutzenden selber und daher mit ihrer Einwilligung in die Internetprofile geladen.
– Privatpersonen erhalten einen umfassenden Zugriff auf die Personendaten anderer Privatpersonen. Daraus können verschiedene Risiken entstehen.

Umgang mit Personendaten in SNS

SNS bergen viele Vorzüge für die Gesellschaft, so zum Beispiel die Möglichkeit, Networking zu betreiben, Kontakte über Landesgrenzen hinaus zu knüpfen oder eigene Inhalte zu publizieren. Es ist daher nicht die Absicht dieser Erläuterungen, SNS grundsätzlich zu verurteilen. Das Ziel ist vielmehr die Sensibilisierung der Behörden und User für einen datenschutzkonformen Umgang mit Personendaten in sozialen Netzwerken, denn Social Networking Services sind zwar meistens gratis, aber sie sind keine gemeinnützigen Einrichtungen. Es findet ein «Handel» statt:

Dienstleistungen für Benutzerinnen und Benutzer im Tausch gegen deren Daten. Hinter den Portalen steckt eine geballte Marktmacht, internationale Unternehmungen, die unter dem Druck von Investoren und Aktionären wachsende Profite generieren müssen. Das einzige, was ein Social Networking Service ihren Investoren anzubieten hat, sind Personendaten – und der Börsenwert einer SNS spricht Bände über deren Wert.

Risiken und Gefahren

Die Benutzung von sozialen Netzwerken birgt verschiedene bekannte Gefahren. Übeltäter können sich dabei die spezifischen Voraussetzungen der SNS zunutze machen. Zu diesen Voraussetzungen gehört unter anderem eine Neubesetzung der Begriffe Vertrauen und Vertraulichkeit. Wo Freundschaft zunehmend quantitative Aspekte hat, ist es unter Vorspiegelung falscher Tatsachen oder gar mit Hilfe einer falschen Identität einfach, zum «Freund» von jemandem zu werden und auf diese Weise in den Besitz von Informationen zu gelangen, die einem das Gegenüber in einem Gespräch von Angesicht zu Angesicht vielleicht nicht mitteilen würde. Die Behauptung solcher Netzwerke, man verlagere einzig die alltägliche Kommunikation unter Freunden ins Internet, suggeriert eine Intimität, die in Wirklichkeit nicht gegeben ist, zumal wenn die Zugangshürden zum Netzwerk niedrig sind.

Wer SNS unvorsichtig und ohne Vorkehrungen benutzt, setzt sich folgenden Risiken aus:

Benutzerkonten, Profile

Konten können praktisch nie unwiderruflich gelöscht werden. Zum einen werden Profile z. T. nur «deaktiviert» statt gelöscht. Zum anderen hinterlassen aktive Benutzende viele zusätzlichen Informationen auf anderen Seiten des Netzwerks. Diese allumfassend zu löschen ist praktisch unmöglich. So verlieren Benutzerinnen und Benutzer die Kontrolle über ihre Daten.

Persönliche Daten

Das Internet kennt kein Vergessen: Benutzerprofile können von anderen Usern heruntergeladen und gespeichert werden. Die Löschung des Ursprungsprofils wird dadurch quasi nutzlos gemacht, denn die Daten bleiben immer irgendwo erhalten. Es entsteht eine Unzahl von privaten Datensammlungen, welche das Bewirtschaften der Daten durch Kategorisierung nach bestimmten Kriterien mittels Suchfunktion ermöglichen. Dadurch wächst die Gefahr, dass diese Daten anders eingesetzt werden, als ursprünglich beabsichtigt. Wenn sie ausserhalb von SNS bekannt gemacht werden, könnten sie der betroffenen Person erheblich schaden.

Metadaten

Die SNS-Provider haben Zugriff nicht nur auf die Personendaten, sondern auch auf die Metadaten. Bei vielen SNS-Anbietenden ist nicht klar, was mit Metadaten wie z. B. Verbindungsdauer, geografische Herkunft der IP-Adresse, Verweildauer und Bewegungen auf der Site etc. geschieht. Personen- und Metadaten zusammen können ausführliche Persönlichkeitsprofile ergeben.

Fotos, Bilder
Fotos mit erkennbaren Personen und zugeordneten Namen dienen der eindeutigen Identifikation der Abgelichteten. Mit spezieller Gesichtserkennungs-Software können SNS und andere Plattformen nach spezifischen Personen abgesucht werden. Diese können dann auch da, wo sie anonym bleiben wollen, z. B. auf einer Dating-Website, identifiziert oder mit Hilfe des Fotos auf der SNS mit ihrem Lebenslauf auf einer Firmenwebsite in Verbindung gebracht werden.

CBIR
In eine ähnliche Richtung geht die Gefahr des CBIR (content based image retrieval): Die automatische Wiedererkennung von Merkmalen im Hintergrund eines Bildes z. B. kann ein spezifisches Gemälde oder Haus zur geografischen Lokalisierbarkeit einer Fotosituation führen und die Bekanntgabe der Adresse Stalking oder andere kriminelle Handlungen zur Folge haben.

Verlinkungen
Einige SNS erlauben weitgehende Verlinkungen mit Profilen oder E-Mail-Adressen von Drittpersonen – durchaus auch solchen, die keine Mitglieder des Netzwerks sind – notabene, ohne deren Erlaubnis einzuholen. Dies kann zur Gefahr für die Privatsphäre jeder Person werden.

Single Sign On
Nutzende mehrerer SNS können die Bewirtschaftung ihrer Postfächer vereinfachen, indem sie alle in einer einzigen Webapplikation eingeben. Auf diese Weise können sie mit einem Benutzernamen und einem Passwort alle aktuellen Nachrichten der eigenen Profile auf einen Blick einsehen, was praktisch sein mag, jedoch Sicherheitsbedenken weckt.

Kriminelle Handlungen

Bei den meisten SNS sind die Registrationshürden sehr niedrig: Man macht einige Angaben zur Person, die nicht verifiziert werden und also erfunden sein können. Einmal drin, ist es unter Umständen sehr einfach, Kontakte zu schliessen und in die «Freundeskreise» anderer aufgenommen zu werden. Das birgt Gefahren der Infiltration dieser Communities zu verschiedenen fragwürdigen oder gar kriminellen Zwecken:

Identitätsdiebstahl

Identitätsdiebstahl wird einfach gemacht: Man legt sich ein Profil mit dem Namen einer bekannten Person an und profitiert von deren Berühmtheit – oder schädigt ihren Ruf durch bösartiges Verhalten. Gleichermassen kann man ein Profil im Namen einer Person aus Schule oder Nachbarschaft eröffnen und ihr schaden, indem man sie lächerlich macht oder in ihrem Namen Bösartigkeiten verschickt.

Zu den kriminellen Formen von Datenmissbrauch zählen das sog. Phishing, der Datendiebstahl zu kriminellen Zwecken, ferner das Cyberstalking und das Cyberbullying.

Phishing

Mit Phishing bezeichnet man den Datendiebstahl mit Hilfe von gefälschten E-Mails und Webformularen: Der Benutzer wird in den Glauben versetzt, er gäbe seine Daten in ein vertrauenswürdiges Formular ein (z. B. seiner Bank), in Wirklichkeit liefert er seine persönlichen Daten (z. B. Logins, Passwörter, TAN- und PIN-Codes etc.) an einen Datendieb.

Cyberstalking
Cyberstalking ist ein altes Phänomen neu verpackt: Die elektronischen Kontaktmöglichkeiten der SNS können böswillig dazu benutzt werden, jemanden zu bedrängen. Ausserdem kann die Menge an Daten, die die Benutzerinnen und Benutzer über sich selber bekannt geben, durchaus dazu führen, dass jemand die Adresse seines Opfers herausfindet, seine Lebensgewohnheiten kennen lernt und die Person in der wirklichen Welt verfolgen kann.

Cyberbullying
Auch Cyberbullying ist die Internet-Version eines in der Realität seit längerem bekannten Phänomens. Der Angreifer kann sich hinter einem gefälschten Profil verstecken, anonym bleiben und dabei die Möglichkeiten nutzen, die SNS bieten, um jemanden bösartig zu belästigen oder zu demütigen. Dies kann erst noch für andere Mitglieder der Community sichtbar getan werden, was den Schaden für das Opfer vergrössert.

Empfehlungen

Benutzerinnen und Benutzer
- Benutzen Sie verschiedene Logins und Passwörter für verschiedene Dienste.
- Wählen Sie in Ihrem Profil bei Ihren eigenen Einstellungen datenschutzkonforme Optionen. Geben Sie Ihre Informationen und Fotos nur für einen beschränkten Personenkreis frei. Stellen Sie heikle Inhalte nicht ins Internet.
- Seien Sie vorsichtig bei der Veröffentlichung Ihrer Personendaten (Name, Adresse, Telefonnummer) und anderer persönlicher Informationen (z. B. politische Überzeugungen) auf einer SNS. Benutzen Sie Pseudonyme.

– Fragen Sie sich vor der Veröffentlichung immer, ob Sie in einem Bewerbungsgespräch mit den entsprechenden Daten konfrontiert werden möchten – und zwar auch noch in zehn Jahren.
– Respektieren Sie die Privatsphäre Dritter, veröffentlichen Sie weder deren Personendaten noch beschriften Sie Fotos mit deren Namen.
– Informieren Sie sich über die Anbietenden des Portals und wie die Privatsphäre der Nutzenden gewährleistet wird. Hat der Dienst ein Datenschutz- oder Sicherheitsgütesiegel?
– Lesen Sie die AGB der Anbietenden. Beobachten Sie das Verhalten des Anbietenden kritisch.

Schulleitungen

– Benutzerinnen und Benutzer von Social Networking Services sollen mit Kampagnen für die damit verbundenen Gefahren sensibilisiert werden.
– Vorsicht mit Verboten: Statt die Benutzung von SNS zu verbieten, sollten Schulen sie (partiell) zulassen; auf diese Weise wird das Social Networking nicht gänzlich unkontrolliert von statten gehen. Zudem könnte die Aufklärung von Lernenden, Lehrkräften und Eltern damit einhergehen.

Europäische Informationen zum Datenschutz

Verschiedene europäische Datenschutzgremien haben sich bereits eingehend mit der Thematik der sozialen Netzwerke befasst.

Weitere Informationen finden Sie unter:

→ European Network and Information Security Agency ENISA. Position Paper No. 1: Security Issues and Recommendations for Online Social Networks (PDF).
Editor: Giles Hogben, October 2007.

→ Bericht und Empfehlung zum Datenschutz in sozialen Netzwerkdiensten «Rom Memorandum», März 2008 (PDF)

E-Mail

Adressfelder
Oft landen im elektronischen Postfach E-Mails, bei denen sämtliche Empfängerinnen und Empfänger sichtbar sind, weil ihre Adressen im «An»- oder im «Cc»-Feld eingefügt wurden. Dies kann aus Transparenzgründen durchaus sinnvoll sein, etwa innerhalb eines Projekts mit verschiedenen Beteiligten oder in ähnlichen Konstellationen, wo sich die Empfänger bereits kennen. Je nach Inhalt und Situation kann eine solche umfassende Empfängerbekanntgabe jedoch heikel sein, insbesondere, wenn sich die Empfänger gegenseitig nicht kennen. In solchen Fällen muss der Absender die «Bcc»-Funktion (blind carbon copy) verwenden. Auf diese Weise erhalten die einzelnen Empfänger keine Kenntnis, wer die Meldung ebenfalls bekommen hat.

Empfehlung
Empfängeradressen beim E-Mail-Versand an Personen, die sich gegenseitig nicht persönlich kennen, immer im Feld «Bcc» eintragen.

Spam- und Phishing-Risiko
Bedenken Sie zudem, dass jede Verbreitung von E-Mail-Adressen das Spam-Risiko und das Risiko für Phishing-Attacken erhöht: Dabei versetzt ein gefälschtes E-Mail, welches irgendwelche Instruktionen und Weblinks enthält, den Empfänger in den Glauben, er kommuniziere mit einem vertrauenswürdigen Absender.

Empfehlung
E-Mails, welche Instruktionen und Weblinks enthalten, sollten Sie ignorieren.

Blogs

Das Datenschutzgesetz verbietet jede Preisgabe von Daten über Drittpersonen ohne vorherige schriftliche Einwilligung der Betroffenen.

Empfehlung

Wenn Sie auf einem fremden Blog Informationen über ihre eigene Person finden, die Sie entfernt wissen wollen, kontaktieren Sie dazu in erster Linie die Autorin, den Autor per Kontaktformular oder E-Mail. Nützt das nichts, nehmen Sie Kontakt auf mit dem Blog-Provider. Publizieren Sie in keinem Fall einen Kommentar zu einer ihre Person betreffenden unerwünschten Information. Ein Kommentar wäre kontraproduktiv, weil er bei der Blog-Leserschaft für mehr Aufmerksamkeit für die unerwünschte Information sorgen würde.

Beim persönlichen Blog ist aber auch die Versuchung besonders gross, Informationen über die eigene Person preiszugeben, ohne dass man sich der Gefahren bewusst ist, die damit verbunden sind. Die Preisgabe von Informationen über die eigene Person ist zwar datenschutzrechtlich unbedenklich, weil sie ja freiwillig erfolgt, aber sie kann dennoch die im Zusammenhang mit sozialen Netzwerken erwähnten negativen Folgen für die eigene Person haben.

Verhaltensregeln

Die folgenden Verhaltensregeln schützen weitgehend vor eventuellen negativen Folgen von persönlichen Blogs:

– Um sich vor zu viel Publizität Ihres privaten Blogs zu schützen, beschränken Sie Ihre Leserschaft. Nutzen Sie dazu die verschiedenen Möglichkeiten, Ihren ganzen Blog oder bestimmte Einträge mit Passwörtern zu schützen oder den Zugriff darauf nur bestimmten Hosts zu erlauben.

- Verwenden Sie immer Pseudonyme und geben Sie keine Einzelheiten bekannt, welche Rückschlüsse auf ihre Persönlichkeit, ihre Gewohnheiten, ihren Wohn- oder Aufenthaltsort, ihren Arbeitgeber etc. erlauben.
- Verwenden Sie Anonymisierungstechniken. Z. B. bietet Invisiblog.com ein kostenloses anonymes Blog-Hosting an. Um zu verhindern, dass Ihre IP-Adresse identifiziert werden kann, verwenden Sie das TOR-Netzwerk (vgl. dazu: → TOR auf Wikipedia). Es gibt auch etliche Software-Anbietende, die sich auf Anonymisierungssoftware spezialisiert haben, wie z. B. → anonymizer.com.
- Verwenden Sie Ping-Server, wenn Sie anonym bleiben möchten, während Sie Ihren Blog verschiedenen Suchmaschinen zuspielen wollen. Pingomatic.com bietet einen entsprechenden Dienst an.
- Verhindern Sie, dass Suchmaschinen Ihren Blog finden. Verwenden Sie dazu ein Robots Text File (robots.txt).
- Registrieren Sie Ihren Domainnamen anonym. Z. B. bietet die Online Policy Group (OPG) eine anonyme Registrierung an.

Tipps zur Anonymisierung und Verschlüsselung von Daten

Wer will, bewegt sich im Internet ohne Probleme anonym, indem er seine Daten grundsätzlich nur verschlüsselt überträgt.

Surfen: Nutzt man das Tor-Netzwerk (→ torproject.org), werden alle Daten verschlüsselt.

Tauschbörsen: Up- und Downloads auf Tauschbörsen lassen sich über den Gratisdienst «Bit Blinder» (→ bitblinder.com) anonymisieren. Es gibt auch kostenpflichtige Anonymisierungsdienste wie Torrent Privacy (→ torrentprivacy.com).

E-Mail: E-Mails lassen sich bei jedem ernsthaften Anbietenden per «https:» sicher übertragen. Per Pretty Good Privacy (PGP) verschlüsselt man die Texte.

Quelle: Christian Bütikofer, Tagesanzeiger 18.07.2009

Digitale Kameras, Handykameras

Unerlaubte Bild- und Tonaufnahmen

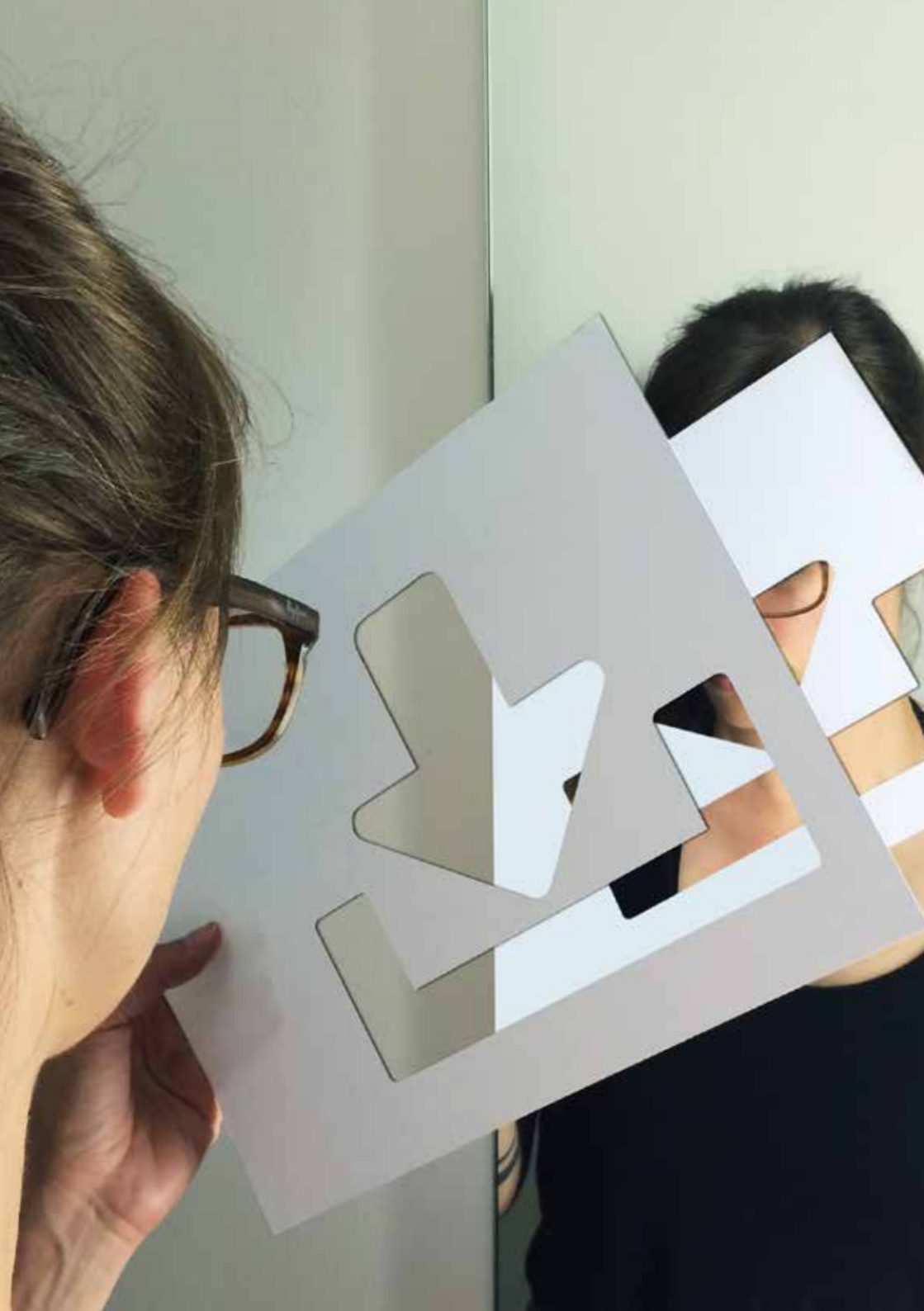
Schülerinnen und Schüler sowie deren Eltern unterstehen als Privatpersonen dem eidgenössischen Datenschutzgesetz. Dieses verbietet Bild- und Tonaufnahmen, welche nicht durch eine persönliche Einwilligung, ein Gesetz oder ein überwiegendes privates oder öffentliches Interesse gerechtfertigt sind. Bild- und Tonaufnahmen verletzen in der Regel Persönlichkeitsrechte, insbesondere wenn solche Aufnahmen mit Kommentaren kombiniert im Internet erscheinen (z. B. auf Websites oder Blogs von Schülerinnen oder Schülern). Schülerinnen und Schüler sind deshalb von den Lehrpersonen und den Schulleitungen darauf hinzuweisen und dass darüber hinaus üble Nachrede, Verleumdung oder Beschimpfung strafbare Handlungen sind.

Aufnahmen durch die Eltern an Schulanlässen

Aufnahmen durch die Eltern an Schulanlässen (Feste, Theater, Sportveranstaltungen, Besuchstage in der Schule oder in Landschulwochen, etc.) betreffen das Rechtsverhältnis zwischen dem aufgenommenen Kind (bzw. dessen Eltern) und der aufnehmenden Person. Es handelt sich somit primär um eine privatrechtliche Angelegenheit. Soweit Eltern über den Anlass, welcher öffentlich oder für andere Eltern zugänglich ist, informiert sind und solange Lehrpersonen keine gravierenden Rechtsverletzungen feststellen (z. B. wenn Eltern andere Kinder durch Aufnahmen bedrängen), besteht keine Pflicht, bei Aufnahmen durch Eltern einzuschreiten. Es ist grundsätzlich Sache der Gefilmten oder Fotografierten (bzw. deren Eltern), ihre Rechte wahrzunehmen und sich gegen eine widerrechtliche Aufnahme zu wehren.

Unangekündigte Einzelbesuche in der Klasse

Bei unangekündigten Einzelbesuchen in der Klasse sollten Aufnahmen unterbleiben, da Eltern hier im Gegensatz zu Schulanlässen nicht über die Aufnahmen informiert sind und ihre Rechte so nicht wahrnehmen können. Aus datenschutzrechtlicher Sicht können Betroffene bei unerlaubten Bild- und Tonaufnahmen gerichtliche Massnahmen zum Schutz der Persönlichkeit ergreifen. In krassen Fällen ist es zulässig, die unverzügliche Löschung der Aufnahmen zu verlangen und bei einer Weigerung die Löschung selbst vorzunehmen.



Schulverwaltung, ICT und Datenschutz

Das Kapitel richtet sich in erster Linie an Schulleitungen. Es erläutert die Grundsätze des Datenschutzrechts und macht insbesondere auf die datenschutzrechtlichen Aspekte im Zusammenhang mit der Verwaltung der persönlichen Daten von Lernenden und Lehrenden unter Verwendung von webbasierten Technologien aufmerksam. Ganz am Schluss folgt ein eher technisches Kapitel zum Thema WLAN und Sicherheit.

Datenschutz und Amtsgeheimnis

Als Mitarbeitende von öffentlichen Anstalten üben Lehrpersonen und Schulleitungen Funktionen im Dienst der Öffentlichkeit aus. Sie gelten deshalb als Behördenmitglieder und unterstehen in dieser Funktion den Bestimmungen des jeweiligen kantonalen Datenschutzgesetzes. Im Übrigen verpflichten auch die strafrechtlichen Regeln über das Amtsgeheimnis (Art. 320 StGB) die Lehrpersonen zur Achtung der Persönlichkeit der Schülerinnen und Schüler.

Amtsgeheimnis

Die strafrechtlichen Regeln über das Amtsgeheimnis verpflichten Mitarbeitende von öffentlichen Anstalten, Amtsgeheimnisse nicht bekannt zu geben. Ein Amtsgeheimnis ist eine nicht allgemein bekannte Tatsache, welche ein Behördenmitglied in der Ausübung seiner Funktion erfahren hat. Die Regeln über das Amtsgeheimnis sind einerseits umfassender als die Datenschutzregeln, weil dazu auch Nicht-Personendaten

(z. B. Budgetfragen einer Schule) gehören. Andererseits haben sie einen engeren Anwendungsbereich, weil sie nur die Bekanntgabe von Geheimnissen und nicht auch die Erhebung, Aufbewahrung, Vernichtung etc. von Daten regeln.

Lehrpersonen sind also verpflichtet «Geheimnisse», die sie in Ausübung ihrer Tätigkeit erfahren haben, nicht bekannt zu geben. Die Bekanntgabe kann jedoch durch eine gesetzliche Ermächtigung oder Pflicht gerechtfertigt sein.

Berufsgeheimnis

Vom Amtsgeheimnis ist das Berufsgeheimnis gemäss Art. 321 des Strafgesetzbuches zu unterscheiden. Es soll zwar auch «Geheimnisse» schützen, gilt aber nicht für Behördenmitglieder, sondern für besondere Berufsgattungen, insbesondere Geistliche, Rechtsanwälte, Notare, Ärzte, Zahnärzte, Apotheker, Hebammen. Es gibt Personen, die beiden Geheimnispflichten unterstehen, z. B. Schulärzte.

Kantonale Datenschutzgesetze

Die kantonalen Datenschutzgesetze bestimmen, wie die kantonalen Behörden mit Personendaten umzugehen haben. Geregelt werden Erhebung, Aufbewahrung, Veränderung, Verknüpfung, Bekanntgabe oder Vernichtung von Personendaten. Daten ohne Personenbezug fallen nicht in den Anwendungsbereich der Gesetze. Verletzten Mitarbeitende von öffentlichen Anstalten die gesetzlichen Bestimmungen, so kann die betroffene Person per Gesuch verlangen, dass die fehlerhaften oder widerrechtlich erhobenen Daten berichtigt oder gelöscht werden. Ausserdem kann eine Verletzung des Datenschutzrechts (z. B. widerrechtliche Bekanntgabe von Personendaten oder der Verlust von aufzubewahrenden Personendaten) intern zu disziplinarischen Massnahmen führen (z. B. Verweis).

Entsteht durch die Verletzung zusätzlich ein Schaden, kann dies Schadenersatzpflichten der Schule (in der Regel haftet die Gemeinde) oder – bei vorsätzlich oder grobfahrlässig herbeigeführten Schäden – der Lehrperson begründen.

Daten zum persönlichen Gebrauch der Lehrperson
Personendaten, welche von einer Lehrperson ausschliesslich für den persönlichen Gebrauch bearbeitet werden, fallen nicht unter das Datenschutzgesetz. Es handelt sich dabei um persönliche Arbeitsmittel der Lehrperson wie Handnotizen zur Vorbereitung eines Elterngesprächs oder Agenda-Einträge. Der Ausschluss dieser Daten vom Datenschutzgesetz führt dazu, dass betroffene Personen kein Einsichtsrecht in diese Daten haben. Er bedeutet jedoch keineswegs, dass diese Daten bekannt gegeben werden. Auch persönliche Arbeitsmittel müssen demnach vor dem Zugriff Dritter geschützt werden und dürfen nicht achtlos herumliegen gelassen werden. Enthält beispielsweise eine Gesprächsnotiz heikle Informationen über einen Schüler, sollte sie in einem verschlossenen Pult oder Schrank aufbewahrt werden. Insbesondere gehören auch die Lernkontrollen zu den Personendaten von Schülerinnen und Schülern, solange sie ihnen zugeordnet werden können. Wird der Name und alle weiteren Elemente, welche eine Zuordnung zu einer bestimmten Schülerin oder einem bestimmten Schüler erlauben würden, entfernt, handelt es sich nicht mehr um Personendaten.

Grundsätze des Datenschutzrechts

Die Bestimmungen in den kantonalen Datenschutzgesetzen richten sich an sämtliche Behörden des Kantons. Sie sind also nicht speziell auf die Bearbeitung von Personendaten in der Schule zugeschnitten. Deshalb ist es wichtig, die Grundsätze des Datenschutzgesetzes zu kennen. Aus ihnen müssen konkrete Lösungen für den Schulalltag abgeleitet werden.

Rechtmässigkeit der Bearbeitung von Personendaten
Die Bearbeitung von Personendaten muss immer rechtmässig sein. Das Datenschutzgesetz unterscheidet dabei zwischen «normalen» und «besonders schützenswerten» Personendaten (siehe oben). Vereinfacht gesagt besteht der Unterschied darin, dass bei der Bearbeitung von «besonders schützenswerten» Personendaten strengere Regeln einzuhalten sind, als bei der Bearbeitung von «normalen» Personendaten.

Bearbeitung von normalen Personendaten
«Normale» Personendaten dürfen bearbeitet werden, wenn
– ein Gesetz (es kann eine Grundlage auf Verordnungsstufe genügen) dazu ermächtigt oder
– die Bearbeitung zur Erfüllung einer gesetzlichen Aufgabe notwendig ist (das heisst, dass die Erfüllung einer gesetzlichen Aufgabe ohne die beabsichtigte Datenbearbeitung erheblich behindert würde).

Bearbeitung von besonders schützenswerten Personendaten
«Besonders schützenswerte» Personendaten dürfen nur bearbeitet werden, wenn zusätzlich
– ein Gesetz (hier ist eine Grundlage auf Gesetzesstufe notwendig) dies klar vorsieht oder
– die Erfüllung einer gesetzlichen Aufgabe die Datenbearbeitung zwingend erforderlich macht (das heisst, dass die Erfüllung einer gesetzlichen Aufgabe ohne die beabsichtigte Datenbearbeitung verunmöglicht würde) oder
– die betroffene Person ausdrücklich zugestimmt hat.

Grundsatz der Zweckbindung
Die nach den oben dargelegten Regeln erhobenen Daten aus dem Schulbereich dürfen grundsätzlich nur für Zwecke, für welche sie beschafft worden sind oder mit welchen Schülerinnen und Schüler oder Eltern rechnen müssen, bearbeitet werden. In der Schule

ergeben sich diese Zwecke aus den oben erwähnten Aufgaben des Kindergartens und der Volksschule. Es ist deshalb beispielsweise grundsätzlich davon abzusehen, Klassenlisten für kommerzielle Zwecke herauszugeben.

Grundsatz der Verhältnismässigkeit
Aus diesem Grundsatz folgt einerseits, dass Personendaten, wie oben bereits erwähnt, nur bearbeitet werden dürfen, wenn dies zur Erfüllung einer gesetzlichen Aufgabe notwendig ist. Ein Datensammeln auf Vorrat (z. B. Erhebung von Daten, für welche zum Zeitpunkt der Erhebung noch gar kein Zweck ersichtlich ist) ist illegal. Andererseits verlangt der Grundsatz der Verhältnismässigkeit, dass unter verschiedenen Möglichkeiten der Datenbearbeitung stets diejenige gewählt werden muss, welche den mildesten Eingriff in die Persönlichkeitsrechte der betroffen Person darstellt.

Grundsatz von Treu und Glauben
Aus dem Grundsatz von Treu und Glauben folgt, dass die Datenbearbeitung erkennbar und transparent sein muss. Eine heimliche Datenbearbeitung ist somit untersagt. Die Schülerinnen und Schüler sowie die Eltern müssen ohne besondere Anstrengung erkennen können, ob und welche Personendaten über sie bearbeitet werden. Personendaten sind deshalb in der Regel bei den betroffenen Schülerinnen und Schüler oder Sorgeberechtigten und nicht bei einer anderen Privatperson oder Behörde zu beschaffen.

Grundsatz der Richtigkeit
Dieser Grundsatz gibt Schülerinnen und Schüler sowie Eltern das Recht, unrichtige Personendaten über sie korrigieren oder vernichten zu lassen.

Datensicherheit
Wer Personendaten bearbeitet, ist auch für deren Sicherung verantwortlich.

Anforderungen an die Einwilligung zur Datenbearbeitung

Einwilligung kann eine Grundlage zur Rechtmässigkeit von Datenbearbeitungen sein. Allerdings sollte die Einwilligung zur Datenbearbeitung jeweils nur eine ganz bestimmte, zeitlich und örtlich eng umschriebene Situation betreffen und nie pauschal erfolgen oder eine zeitlich unbefristete Datenbearbeitung erlauben. Die betroffene Person ist in der Regel die Schülerin oder der Schüler. Da eine Einwilligung nur von einer urteilsfähigen Person erteilt werden kann, ist zunächst zu klären, unter welchen Bedingungen Schülerinnen und Schüler urteilsfähig sind. In einem zweiten Schritt sind die Anforderungen an die Form der Einwilligung zu prüfen. Urteilsfähig im Sinne des Zivilgesetzbuches ist, wer nicht wegen seines Kindesalters oder infolge von «Geisteskrankheit, Geistesschwäche, Trunkenheit oder ähnlichen Zuständen» ausserstande ist, vernunftgemäss zu handeln. Dies bedeutet, dass Kinder oder Jugendliche urteilsfähig sind, wenn sie sich einen eigenen Willen bilden und gemäss diesem Willen handeln können. Das Gesetz kennt keine feste Altersgrenze. Je nach Entwicklungsstufe des heranwachsenden Kindes reicht sein Erfahrungshorizont unterschiedlich weit. Schülerinnen und Schüler des Kindergartens und der Volksschule sind in der Regel zwischen 4 und 16 Jahre alt. In dieser Zeitspanne variiert die Fähigkeit, einen eigenen Willen zu bilden und diesem Willen entsprechend zu handeln erheblich. Auch unter Gleichaltrigen kann diese Fähigkeit sehr unterschiedlich ausgebildet sein.

Grundsätzlich kann aber Folgendes gesagt werden

Da es oft sogar für Erwachsene schwierig ist, die Konsequenzen einer Datenbearbeitung abzuschätzen, ist dies für Kinder umso schwieriger. Darum kann ihnen bezüglich der Bearbeitung von «besonders schützenswerten» Personendaten sowie bezüglich der Bearbeitung von «normalen» Personendaten, welche ihre Persönlichkeitsrechte gefährden und nur

schwer abschätzbare Folgen nach sich ziehen können, höchstens gegen Ende der Volksschulzeit Urteilsfähigkeit zugesprochen werden. Vorher empfiehlt es sich, die Einwilligung bei den Erziehungsberechtigten einzuholen. Nur in sehr klaren und einfachen Fällen kann ein Kind die Konsequenzen einer Datenbearbeitung abschätzen und sich diesbezüglich einen eigenen Willen bilden.

Einwilligungen

Bei Einwilligungen unterscheidet man mündliche von schriftlichen und ausdrückliche von stillschweigenden Einwilligungen. Werden «normale» Personendaten, von welchen keine erhebliche Gefährdung für die betroffenen Personen ausgeht, bearbeitet, kann eine stillschweigende Einwilligung genügen. Eine stillschweigende Einwilligung wird angenommen, wenn gegen eine reglementarisch vorgesehene oder allgemein bekannt gegebene Datenbearbeitung kein Einspruch erfolgt. Aus Beweisgründen sollten Einwilligungen aber trotzdem wenn immer möglich schriftlich eingeholt werden.

Persönliche Daten weitergeben

Grundsätzlich ist eine Datenweitergabe nur insoweit erlaubt, als die betroffene Gemeinde dies in ihrem Datenschutzreglement ausdrücklich gestattet. Kantonale Muster-Datenschutzreglemente sehen in der Regel ein Verbot der Datenbekanntgabe für kommerzielle Zwecke vor. Es gibt allerdings Gemeinden, in welchen Gemeindeerlasse derartige Datenbekanntgaben ausdrücklich erlauben. Liegt ein solcher Gemeindeerlass vor, ist die Bekanntgabe gestattet (z. B. Art. 3 Abs. 1 Datenschutzreglement der Gemeinde Thun).

Listenauskünfte

Listenauskünfte sind systematisch geordnete Daten, z. B. eine Liste der Namen, Adressen oder E-Mail-Adressen aller Schülerinnen und Schüler einer Schule oder aller Erziehungsberechtigten der Schülerinnen und Schüler einer Schule. Sie dürfen grundsätzlich nur weiter gegeben werden, wenn die zuständige Gemeinde genau dies in einem Datenschutzreglement ausdrücklich erlaubt. Allerdings sind die betroffenen Personen vor der erstmaligen Bekanntgabe zu informieren, um ihnen die Geltendmachung überwiegender Interessen zu ermöglichen. Dieses Vorgehen empfiehlt sich insbesondere dann, wenn der Verdacht besteht, dass die Personendaten missbraucht werden könnten (z. B. für Marketing). Benötigen Sie für eine Datenweitergabe das Einverständnis der Erziehungsberechtigten oder der Schülerinnen und Schüler, dann holen Sie aktiv eine ausdrückliche, schriftliche Zustimmung ein. Verwenden Sie keine Formulierungen wie «ohne Ihren Gegenbericht bis … nehmen wir an, dass Sie einverstanden sind». [BL: Merkblatt Datenschutz]

Anfragen für kommerzielle Zwecke

Anfragen – insbesondere von Seiten von Webservice-Anbietenden – ist mit grösster Zurückhaltung zu begegnen. In jedem Fall sind die AGBs der Anbietenden von Web-Diensten (z. B. von Software-as-a-Service-Providern) genau zu lesen, denn was sich im Werbeprospekt als attraktives Angebot für die Schule präsentiert, kann mit Bedingungen verbunden sein, die unerwünschte Abhängigkeiten schaffen oder datenschutzrechtlich bedenklich sind.

Schulwebsites

Wer Daten über Schülerinnen und Schüler oder Lehrpersonen auf dem Internet zugänglich macht, bearbeitet damit Personendaten. Es sind demnach auch hier die bereits erwähnten Prinzipien zu beachten. Daten, die auf dem Internet veröffentlicht werden, sind weltweit abrufbar und können für verschiedenste Zwecke gebraucht und missbraucht werden. Insbesondere mit Bildern sollte deshalb sehr vorsichtig umgegangen werden. Ausserdem sind die Anforderungen an die Sicherheit im Internet einzuhalten.

Es sind Personen zu bezeichnen, welche für die Sicherheit der Daten verantwortlich sind. Insbesondere für diese Personen empfiehlt sich die Lektüre der Broschüre → «Der sichere Umgang mit Informations- und Kommunikationsgeräten».

Richtlinien für Schulwebsites

In der Regel kann problemlos veröffentlicht werden:
Informationen ohne Personenbezug:
- Schulagenda
- Schulorganisation
- Leitbilder
- Adressen schulnaher Institutionen
- Schulordnungen

Reportagen ohne Personenbezug:
- Schul- oder Klassenanlässe
- Theateraufführungen
- Schulfeste
- Themenwochen
- Exkursionen

Arbeiten von Schülerinnen und Schülern, sofern sie ihnen nicht zugeordnet werden können

Daten über Schülerinnen und Schüler und Schulpersonal

Generell gilt: Sind Betroffene mit der Veröffentlichung irgendwelcher Personendaten – auch die sogenannt unproblematischen – nicht einverstanden oder ziehen sie ihre Einwilligung später zurück, ist ihrem Recht auf Beseitigung umgehend zu entsprechen und der fragliche Inhalt unverzüglich von der Website zu entfernen.

Unproblematische Daten

In der Regel sind folgende Daten unproblematisch:

- Familiennamen
- Vornamen
- Funktionen

Vorgängige, ausdrückliche und freiwillige Einwilligung erforderlich

Folgende sensiblen Personendaten dürfen grundsätzlich nicht ohne vorgängige, ausdrückliche und freiwillige Einwilligung veröffentlicht werden:

- Privatadressen
- E-Mail-Adressen
- Bilder von Personen, wenn die Personen identifizierbar sind
- Angaben zu Hobbys und Lieblingsfächern
- Arbeiten von Schülerinnen und Schülern mit Personenbezug

Sensible Daten

Trotz vorgängiger, ausdrücklicher und freiwilliger Einwilligung sollte darauf verzichtet werden, die folgenden Daten auf einer Schulwebsite zu veröffentlichen:

- Private Adressen
- Telefonnummern
- E-Mail-Adressen
- Bilder, auf denen Personen identifizierbar sind

Links
Links dürfen nicht auf widerrechtliche Seiten verweisen. Das sind Seiten, die z. B. pornographische, rassistische oder ehrverletzende Inhalte aufweisen. Alle Links müssen periodisch darauf hin kontrolliert werden.

Webcams
Auf den Einsatz von Web-Cams zur Übertragung von Bildern identifizierbarer Personen ist zu verzichten.

Kontaktformulare
Stellt eine Website eine Kontaktmöglichkeit via E-Mail oder Webformular zur Verfügung, ist darauf hinzuweisen, dass die Verbindung unsicher ist und vertrauliche Informationen nicht online übermittelt werden sollten.

Aufzeichnung von Besuchen, Cookies
Eine Registrierung der User ist verboten. Setzt die Seite Cookies, ist zu erklären, zu welchem Zweck.

Gästebücher, Foren
Gästebücher und Foren dürfen nicht verwendet werden, wenn Dritte ihre Beiträge ohne vorherige Prüfung durch die Schule direkt auf die Seite eingeben können. Die Schule hat mögliche Verunglimpfungen von Dritten zu verhindern.

Einige Sicherheitshinweise zu WLAN

WLAN steht für «Wireless Local Area Network», zu Deutsch: drahtloses lokales Netzwerk. WLANs dienen insbesondere dazu, den Internetzugang mit mobilen Geräten in Hotels, Restaurants, Bahnhöfen, der eigenen Wohnung oder in Firmen zu ermöglichen. WLANs verbinden Rechner, Drucker, Scanner und andere Geräte und ermöglichen meist auch eine Verbindung ins Internet. Diese Geräte sind durch sogenannte «Access Points» miteinander verbunden. WLAN ist durch die IEEE standardisiert (→ IEEE auf Wikipedia).

Sowohl bei Firmen wie in privaten Haushalten erfreuen sich WLANs heute grosser Beliebtheit, denn sie ermöglichen grosse Flexibilität ohne Kabelsalat bei hohen Übertragungsraten. Die Reichweiten zwischen dem Access Point und den Geräten betragen, je nach Sendeleistung und Mauerbeschaffenheit, wenige Meter bis mehrere Dutzende Meter.

Die nicht von der Hand zuweisenden Vorteile von WLANs machen auf der anderen Seite besondere technische und organisatorische Massnahmen nötig. Denn die Funksignale sind grundsätzlich im Ganzen von einem WLAN abgedeckten Gebiet zugänglich, d. h. also auch für unbefugte Dritte. Zum einen geht es also darum, vertrauliche Daten vor dem Zugriff solcher Drittpersonen zu schützen. Zum anderen sollen Unbefugte auch nicht als Trittbrettfahrer die Bandbreite des WLANs für den Internetzugang schmälern oder diesen gar für illegale Handlungen missbrauchen können.

Sicherheitsmassnahmen

Die Melde- und Analysestelle Informationssicherung MELANI des Bundes schlägt folgende konkrete Datensicherheits- und Datenschutzmassnahmen vor:

- Standardpasswort zur Verwaltung des Access Points ändern.
- Zur Verwaltung des Access Points wenn möglich Kabel, z. B. Ethernet, verwenden und die Funktion für die Verwaltung über Funk ausschalten.
- Mögliche Funktionen für die Fernverwaltung des Access Points über das Internet ausschalten.
- Die Netzwerkidentifikation (SSID) ändern und das Aussenden der Netzwerkidentifikation (SSID Broadcast) ausschalten, damit der Access Point Aussenstehenden verborgen bleibt.
- Die stärkste Verschlüsselung, die vom Access Point und von den Endgeräten unterstützt wird, einsetzen (vorzugsweise WPA 2 oder WPA). Die längste Schlüssellänge bzw. ein starkes Passwort benutzen. Der frühere Standard Wired Equivalent Privacy (WEP) bietet zu wenig Sicherheit und sollte nicht mehr verwendet werden.
- Wenn es im Netzwerk praktikabel und das notwendige Wissen vorhanden ist, statische IP-Adressen anstatt DHCP (Dynamic Host Configuration Protocol) benutzen.
- Den MAC-Filter benutzen, um den Zugang zum WLAN auf die bestimmten Endgeräte im Netzwerk einzuschränken.
- Wenn die Funktion im Access Point vorhanden ist und der Betrieb des Netzwerks nicht dadurch beeinträchtigt wird, Sendeleistung verringern, um die Reichweite des WLANs zu vermindern.
- Das WLAN nur bei Gebrauch einschalten.

Hilfreiche Links zum Thema WLAN

→ MELANI: Funknetzwerke (WLAN)
→ BAG: WLAN
→ Wikipedia: Wi-Fi Protected Access

educa.ch
Schweizer Medieninstitut für Bildung und Kultur
Erlachstrasse 21 | Postfach 612 | CH-3000 Bern 9

Telefon: +41 (0)31 300 55 00
info@educa.ch | www.educa.ch