

Kontrolle, Persönlichkeitsrechte und Datenschutz im digitalen Raum: Rechtliche Informationen für stationäre Einrichtungen der Jugendhilfe

Begriffsklärungen

Datenschutz meint den Schutz von Personendaten und damit verbunden den Schutz der Persönlichkeit und der Grundrechte von Personen. Personendaten sind Daten, sie sich auf eine konkrete Person beziehen. Gesetze zum Datenschutz gibt es im Europäischen Raum, auf Bundesebene und in den Kantonen.

Das schweizerische Zivilgesetzbuch betont die **Persönlichkeitsrechte** von allen Menschen, also auch von Kindern und Jugendlichen. Nach dem ZGB haben alle Menschen in den Schranken der Rechtsordnung die **Fähigkeit für Rechte und Pflichten** und hat jedes Individuum ein Recht auf Unversehrtheit unter anderem in folgenden Persönlichkeitsbereichen:

- Physische Persönlichkeit: Schutz der körperlichen Integrität, Bewegungsfreiheit
- Affektive (emotionale) Persönlichkeit: Schutz vor unmittelbaren und nachhaltigen Beeinträchtigungen im seelisch-emotionalen Lebensbereich
- Soziale Persönlichkeit: Recht auf Geheim- und Privatsphäre, Verschwiegenheit, informationelle Freiheit (u.a.)

(Voll) **handlungsfähig** ist jede Person, die volljährig (d.h. 18-jährig) und urteilsfähig ist.

Urteilsfähig sind Personen, wenn sie in einer konkreten Lebenssituation „vernunftgemäss“ handeln können, d.h. wenn sie die Tragweite des eigenen Handelns begreifen (**Erkenntnisfähigkeit**) und fähig sind, gemäss dieser Einsicht aus freiem Willen vernunftgemäss zu handeln (**Willensumsetzungsfähigkeit**). Auch Personen unter 18 Jahren können in Teilbereichen urteilsfähig sein. Die Urteilsfähigkeit ist immer in Bezug auf eine konkrete Situation zu beurteilen. Eine Person kann in Bezug auf gewisse Handlungen urteilsfähig sein, in Bezug auf andere urteilsunfähig.

Urteilsfähige Minderjährige gelten als **beschränkt handlungsunfähig**. Wenn Kinder und Jugendliche die Folgen eines Entscheids abschätzen können, dürfen sie beispielsweise mit Zustimmung der Eltern Verträge eingehen, selber verdientes Geld (z.B. durch einen Ferienjob) selbständig verwenden und die höchstpersönlichen Rechte ausüben. Urteilsfähige minderjährige Kinder und Jugendliche dürfen also über Persönlichkeitsrechte selbständig entscheiden. Persönlichkeitsrechte von urteilsfähigen Kindern und Jugendlichen beinhalten u.a.: Entscheidung, wer welche persönlichen Informationen über sie erhält (dies schliesst auch die Eltern mit ein), Entbindung vom Arztgeheimnis, Anzeige bei der Polizei, Beitritt zu einem Verein.

Wenn ein urteilsfähiges Kind einerseits seine Persönlichkeitsrechte ausübt, dies aber andererseits in einem engen Zusammenhang mit einer Gefährdung oder einem Schutzbedarf des Kindes steht (z.B. exzessives Spielen von Computerspielen, unbekanntem Personen auf Sozialen Netzwerken persönliche Informationen weitergeben), so stehen die Erziehungsberechtigten und also auch das Wohnheim als (teilweiser) Obhutsinhaber in der Verantwortung. Hier braucht es Güterabwägungen zwischen den Persönlichkeitsrechten des Kindes und dessen Schutzbedarf.

Hintergrundinfo/zum Weiterdenken:

Bei Kindern und Jugendlichen ist die **Gehirnentwicklung** noch nicht abgeschlossen. Insbesondere das Frontalhirn mit seiner hemmenden Funktion ist in der Jugendphase noch nicht vollständig ausgereift. Dies beeinflusst die Sinne, Gefühle, Gedanken und die Persönlichkeit. Teenager haben für einige Jahre keine neuronale «Spass-Bremse» im Kopf. Dies ist eine wichtige Ursache, warum Jugendliche oftmals Schwierigkeiten haben, Regeln und Grenzen zu respektieren, warum sie ihre Emotionen nicht im Griff haben und unausgeglichen sind, und warum sie sich oftmals aus der Sicht der Erwachsenen unvernünftig und nicht adäquat verhalten.

Überblick über Faktenlage

Grundprinzipien des Datenschutzes sind:

- *Rechtmässigkeit*: Es braucht einen Rechtfertigungsgrund, um Daten über eine Person zu erheben, zu bearbeiten oder weiterzugeben.
- *Verhältnismässigkeit*: Es dürfen nur Daten erhoben werden, welche für den Zweck des Auftrags geeignet, notwendig und für die Betroffenen zumutbar sind (d.h. wenn der Zweck gewichtiger ist als mögliche negative Folgen der Datenerhebung). Die Daten dürfen nur solange aufbewahrt werden, wie zur Erfüllung der Aufgabe notwendig. Daten dürfen nur soweit bearbeitet werden, wie es für den Zweck notwendig ist.
- *Transparenz*: Die betroffenen Personen müssen über Art, Umfang und Zweck der Daten informiert werden; sie dürfen jederzeit Auskunft über ihre Daten erhalten und Dateneinsicht nehmen.
- *Treu und Glauben*: Personendaten sollen transparent beschafft und bearbeitet werden. Verboten sind eine Beschaffung ohne Wissen oder gegen den Willen der betroffenen Person oder unter Täuschung der Person (zum Beispiel durch Vorspielen einer falschen Identität).
- *Zweckbindung*: Daten dürfen nur für den Zweck verwendet werden, der bei der Erhebung definiert war, ausser es besteht eine explizite Einwilligung in die neue Verwendung oder eine gesetzliche Datengrundlage.
- *Richtigkeit*: Die Daten sind zu datieren. Sie müssen korrekt und korrigierbar sein.
- *Datensicherheit, Informationssicherheit*: Die Daten sind vor fremdem Zugang zu sichern.

Persönlichkeitsrelevante Daten dürfen erhoben, bearbeitet und weitergegeben werden, wenn einer der folgenden datenschutzrechtlichen Rechtfertigungsgründe vorliegt:

- 1 *Einwilligung*: Wenn die betroffene Person *urteilsfähig* ist, braucht es eine Einwilligung dieser Person. Dabei ist zu beachten: Die Person muss verstehen, was wozu und mit welchen möglichen Folgen erhoben wird; Blankobevollmächtigungen reichen nicht. Ausserdem muss die Einwilligung freiwillig sein: Mögliche Nachteile bei einer Verweigerung müssen im Zusammenhang mit dem Zweck der Datenbearbeitung stehen und verhältnismässig sein. Wichtig: Wenn eine Person bezogen auf einen bestimmten Sachverhalt urteilsfähig ist (wenn sie also die Tragweite des eigenen Tuns abschätzen kann), entscheidet sie darüber grundsätzlich selbständig. Die Urteilsfähigkeit bezieht sich immer auf den aktuellen Sachverhalt. Falls die betroffene Person *nicht urteilsfähig* ist, braucht es eine Einwilligung der gesetzlichen Vertretung. Bei *höchstpersönlichen Themen* (z.B. Liebe und Sexualität) braucht es immer die Zustimmung der betroffenen Person!
- 2 *Gesetzliche Ermächtigung* zur Datenfreigabe resp. -bearbeitung: Eine Informationsbeschaffung oder Informationsweitergabe ist ohne Einwilligung und gegen den Willen der betroffenen Person möglich, wenn dies in Zusammenhang steht mit der Erfüllung eines gesetzlichen Auftrags. Für Wohnheime relevant ist die Meldepflicht gegenüber Kindes- und Erwachsenenschutzinstanzen.

3 Bei überwiegendem privaten oder öffentlichen Interesse, z.B. in akuten Notsituationen

Wenn eine Einrichtung beispielsweise die Surf-Chronik der Kinder und Jugendlichen protokollieren will, so müssen vorliegen: eine Einwilligung der Eltern/der urteilsfähigen Jugendlichen (z.B. über einen Medienvertrag), ein definierter Zweck und ein definiertes Vorgehen, wie mit diesen Daten umgegangen wird (Zugriff, Aufbewahrung, Verarbeitung etc.) sowie notwendige technische Sicherungsmassnahmen vor unbefugtem Zugriff auf die Daten.

Daten dürfen an Dritte nur mit einem Rechtfertigungsgrund weitergegeben werden (siehe oben). Dies beinhaltet auch die Information der Eltern! Diese dürfen bei höchstpersönlichen Themen (z.B. Sexualität) nur mit Einverständnis der Kinder/Jugendlichen oder bei überwiegend privatem oder persönlichem Interesse informiert werden.

Ob Persönlichkeitsrechte verletzt werden, kann nur nach Analyse der konkreten Umstände entschieden werden. In unklaren Fällen gilt der Massstab an Persönlichkeitsrechten, der nach Treu und Glauben in der konkreten Situation normalerweise erwartet werden kann. Bei Einschränkung von Persönlichkeitsrechten muss immer kritisch geprüft werden, ob die jeweiligen Zwecke auch mit weniger einschneidenden Möglichkeiten erreicht werden können.

Bezüglich Einschränkungen von Persönlichkeitsrechten von besonderer Bedeutung ist, was mit einem Heimvertrag, in Reglementen oder in individuellen Vereinbarungen konkret und beweisbar (vertraglich) abgemacht wurde und von den Eltern als gesetzliche Vertreter, aber auch vom betroffenen urteilsfähigen Jugendlichen akzeptiert wurde. Es sind dabei nur Vereinbarungen sinnvoll, welche auch überprüft und durchgesetzt werden können. Auch bei vertraglichen Vereinbarungen muss allerdings die Verhältnismässigkeit der Einschränkung von Persönlichkeitsrechten kritisch geprüft werden.

Avenir Social (Mösch Pavot & Pärli 2013) empfiehlt, den Schutz der Person grundsätzlich höher zu gewichten als das Informationsinteresse der Organisation. Sie empfehlen deswegen folgende Regeln im Umgang mit persönlichen Daten: [Empfehlungen sprachlich vereinfacht]

- den Umfang der Daten genau definieren;
- die Kompetenz der Auskunftserteilung im Voraus für verschiedene mögliche Situationen regeln;
- Melde- und Anzeigepflichten transparent machen;
- die Verantwortung für das Vernichten und Archivieren von Daten regeln;
- ein Verzeichnis über die Daten erstellen inkl. Zweck, Inhalt und Art der Bearbeitung;
- ein Sicherheitskonzept mit Zugriffskontrolle und Zugriffsbeschränkung ausarbeiten;
- die Mitarbeiterinnen und Mitarbeiter über Datenschutzaspekte informieren.

Quelle/zum Weiterlesen:

Curaviva (2015): *Professionelles Handeln im Spannungsfeld von Nähe und Distanz. Eine Handreichung aus Sicht der Praxis und der Wissenschaft.* [Link](#)

okaj zürich, *Kantonale Kinder- und Jugendförderung (2017): Alles was Recht ist: Rechtshandbuch für Jugendarbeitende.* Zürich: Orell Füssli Verlag

Mösch Pavot, Peter, Pärli, Kurt (2013): *Datenschutz in der Sozialen Arbeit: eine Praxishilfe zum Umgang mit sensiblen Personendaten.* Bern: AvenirSocial - Soziale Arbeit Schweiz

Schlussfolgerungen und Empfehlungen für stationäre Einrichtungen der Jugendhilfe

Grundsätze

- Prüfen Sie, ob eine Datensammlung wirklich mit Blick auf die Zielsetzung der Institution notwendig und die Weitergabe von Daten verhältnismässig ist: Suchen Sie nach Wegen, um so wenig Daten wie möglich zu sammeln, diese so kurz wie möglich zu speichern und nur den Personen Zugriff zu geben, welche diese tatsächlich benötigen.
- Stellen Sie sicher, dass eine Einwilligung der Betroffenen zur Datensammlung und -weitergabe vorliegt (ausser es besteht ein gesetzlicher Auftrag, dann reicht eine Information dazu). Dies kann bezüglich digitaler Medien mit einem Medienvertrag erreicht werden.
- Eingriffe in die Persönlichkeitsrechte von Kindern/Jugendlichen (z.B. Blockieren von bestimmten Webseiten), das Speichern von persönlichen Daten (z.B. Protokollieren des Chatverlaufs) und das Weitergeben von Daten (auch an die Eltern!) müssen verhältnismässig und transparent sein. Bezüglich Verhältnismässigkeit braucht es Abwägungen zwischen dem Selbstbestimmungsrecht und Recht auf Privatsphäre der Kinder/Jugendlichen und dem Erziehungsauftrag der Einrichtung. Prüfen Sie immer, ob die Zwecke eines Persönlichkeitseingriffs auch mit weniger Eingriffsintensität erreicht werden können.
- Die Daten sind technisch vor unbefugtem Zugriff zu sichern.
- Diskutieren Sie innerhalb der Einrichtung Spannungsfelder von Persönlichkeitsrechten und dem Erziehungsauftrag der Einrichtung und entwickeln Sie eine gemeinsame, breit abgestützte Haltung. Beziehen Sie dabei nach Möglichkeit auch die Kinder und Jugendlichen mit ein und benutzen Sie dies als Gelegenheit, ergebnisoffen miteinander ins Gespräch zu kommen.
- Regeln zur Nutzung digitaler Medien sind mit (kleineren oder grösseren) Eingriffen in die Persönlichkeitsrechte der Kinder und Jugendlichen verbunden. Entwickeln Sie Medienregeln unter dem Gesichtspunkt, dass diese den Kindern und Jugendlichen Erfahrungs- und Gestaltungsfreiräume gewähren. Lebensweltorientierung bedeutet in diesem Themenbereich, den Zugang der Kinder/Jugendlichen zur digitalen Welt nicht zu stark einzuschränken.
- Medienregeln sollen einfach umsetzbar sein (kontrollierbar, mit realistischen, klar vereinbarten und durchsetzbaren Folgen).
- Die Kinder/Jugendlichen sollten Medienregeln als sinnhaft und angemessen erleben statt als rigide Fremdbestimmung. Darum: Medienregeln demokratisch aushandeln und regelmässig anpassen/revidieren. Hilfreich sind auch Spielräume bei der Umsetzung der Regeln. Dadurch ist ein (in gewissem Umfang) ergebnisoffener Aushandlungsprozess möglich, wodurch die Kinder/Jugendlichen nicht als «Verwaltungsobjekte» adressiert werden, sondern als gleichwertige, handlungsfähige Akteure.

Prüffragen

Avenir Social (Mösch Pavot & Pärli 2013) schlägt folgende Prüffragen vor (adaptiert auf medienbezogene Themen):

Rechtmässigkeit:

- Liegt eine echte Einwilligung zur **Erhebung** von Personendaten vor oder besteht ein gesetzlicher Auftrag?
 - Ist der Zweck der Datenerhebung konkret beschrieben?
 - Ist das Kind, der/die Jugendliche, imstande, die Konsequenzen der Datensammlung zu verstehen und kann damit selber die Einwilligung geben?
 - Kann die Einwilligung verweigert werden? (z.B. Medienvertrag nicht unterschreiben)
 - Bezieht sich der gesetzliche Auftrag explizit auf Medienthemen? (z.B. Isolierung im Strafvollzug)
- Liegt eine echte Einwilligung zur **Weitergabe** von Personendaten vor oder besteht ein gesetzlicher Auftrag? Bei höchstpersönlichen Themen gilt dies auch bezogen auf die Information der Eltern!

Verhältnismässigkeit: Ist die Datenerhebung für den Zweck des Auftrags geeignet, notwendig und für die Betroffenen zumutbar? Besteht ein besonderer Schutzbedarf in Bezug auf Mediennutzung? Gefährdet das Kind, der/die Jugendlich potenziell sich selber oder andere?

Transparenz: Erhalten die Kinder/Jugendlichen und die Eltern genügend Informationen über die Art der erhobenen Daten und den Umgang damit? Können sie Einsicht in die Daten nehmen?

Zweckbindung: Werden die Daten nur für den konkret definierten Zweck verwendet?

Beispiele

Jugendliche und Eltern unterschreiben beim Eintritt in die Einrichtung einen Medienvertrag, in dem steht, dass die Inhalte des Handys kontrolliert werden dürfen und dass die Chronik des Internetverlaufs gespeichert wird.

Es muss klar geregelt sein, welche Daten durch wen mit welchem Zweck angeschaut werden. Hierbei ist die Verhältnismässigkeit zu beachten (z.B. ob ein erhöhtes Missbrauchsrisiko durch die Kinder/Jugendlichen besteht). Die Erziehungsberechtigten müssen diesen Regeln zustimmen. Bei einer Zwangseinweisung reicht es, wenn die Eltern/die Jugendlichen Kenntnis der Regeln haben.

Wenn in der Hausordnung oder in einem Medienvertrag Orte oder Zeiten festgehalten sind, an denen das Handy nicht erlaubt sind, so ist dies rechtlich korrekt, solange die Regelungen verhältnismässig sind (namentlich also gerechtfertigt sind durch ein Schutz- oder Erziehungsinteresse, für welche die Massnahme als angemessen erscheint, z.B. zum Ziel, andere Freizeitaktivitäten nicht zu beeinträchtigen). Das Einziehen von Handys zur Schlafenszeit beispielsweise kann als erzieherische Massnahme oder zum Schutz der Erholung verhältnismässig sein. Das Einziehen von Handys zur Schlafenszeit beispielsweise kann als erzieherische Massnahme oder zum Schutz der Erholung verhältnismässig sein.

Wichtig: Bei einer Kontrolle von Handys durch die Mitarbeitenden könnte der Vorwurf der Datenmanipulation entstehen. Bei Vorfällen, die strafrechtlich relevant sein könnten, die Jugendlichen die Inhalte zeigen lassen. Wenn die Jugendlichen nicht zustimmen, soll das Handy der Polizei zur Überprüfung übergeben werden.

<p>Die Mitarbeitenden haben entdeckt, dass der 15-jährige Sven mehrmals über seinen privaten Laptop Pornos geschaut hat. Sie informieren die Eltern beim nächsten Elterngespräch darüber.</p>	<p>Der Konsum von legaler Pornografie ist in der Schweiz nicht verboten. Also verstösst Sven nicht gegen das Gesetz. Es wäre verboten, wenn die Mitarbeitenden dem 15-jährigen Pornografie zur Verfügung stellen oder ihn bei der Beschaffung unterstützen. Es besteht aber mit Blick auf den Datenschutz und das Recht auf Selbstbestimmung (Persönlichkeitsschutz) keine generelle Grundlage für die Mitarbeitenden, die Tätigkeit von Sven zu unterbinden, ausser wenn Dritte oder er selber entwicklungsgefährdend betroffen sind.</p> <p>Vor diesem Hintergrund ist eine Information der Eltern ohne Einwilligung des Jugendlichen nur dann vertretbar, wenn der Pornokonsum ein entwicklungsgefährdendes Mass angenommen hat. Das kann vor allem auch der Fall sein, wenn es sich um verbotene Formen von Pornografie handelt.</p>
<p>Jessica, 14-jährig, beschwert sich, dass andere Jugendliche der Wohngruppe ohne zu fragen Handyfotos von ihr gemacht haben. Sie ist sich nicht sicher, ob Fotos von ihr auf Snapchat oder Instagram gepostet wurden.</p>	<p>Bei dringendem Verdacht auf einen strafrechtlich relevanten Vorfall können Mitarbeitende das Handy konfiszieren und die Polizei verständigen. Die Betreuungspersonen dürfen das Handy nur mit Einverständnis der Kinder/Jugendlichen überprüfen, ausser wenn in einem Medienvertrag eindeutige und klare Vereinbarungen bestehen, wer aus welchem Grund was einsehen darf, und wenn diese Vereinbarung im konkreten Fall verhältnismässig ist.</p> <p>Bei Vorfällen, die strafrechtlich relevant sein könnten, sollten Fachpersonen die Jugendlichen die Inhalte zeigen lassen. Wenn die Jugendlichen nicht zustimmen, soll das Handy der Polizei zur Überprüfung übergeben werden. Auch hier ist die Entwicklung einer gemeinsamen Haltung wichtig.</p> <p>Im vorliegenden Fall ist eine Überprüfung nicht verhältnismässig, weil wegen unerwünschten Handyfotos kein strafrechtliches Verfahren eingeleitet würde. Wenn Jessica durch die Bilder Schaden zugefügt wurde und sie dafür einen Schadenersatz will, wird dies in einem zivilrechtlichen Verfahren beurteilt.</p> <p>Unabhängig von der Frage der straf- und zivilrechtlichen Relevanz sollte ein solcher Konflikt auf der Wohngruppe bearbeitet werden und gemeinsame Regeln erarbeitet werden.</p>
<p>Eine Einrichtung sperrt bestimmte Webseiten durch eine Sicherheitssoftware.</p>	<p>Eine Sicherheitssoftware, die einzelne Webseiten sperrt, ist rechtlich zulässig. Eine technische Einschränkung des Zugangs zum Internet ersetzt aber nicht die pädagogische Arbeit. Zu überlegen ist, in welcher Weise Themen wie «nicht kindgerechte Inhalte im Internet» pädagogisch bearbeitet werden können.</p>
<p>Eine Einrichtung hat die Regel, dass die Kinder und Jugendlichen ihr Handy jeden Tag zwischen 17.30 und 18 Uhr verwenden dürfen.</p>	<p>Schweizer Jugendliche verwendeten im Jahr 2017 das Handy laut James-Studie jeden Tag während 2.5 Stunden. Eine Reglementierung auf eine halbe Stunde pro Tag ist somit weit entfernt vom durchschnittlichen Handygebrauch Jugendlicher und schliesst sie von «normalen» Kommunikationen aus. Dies ist rechtlich zulässig, entspricht jedoch nicht einer Lebensweltorientierung. Ein sehr enger Rahmen führt auch eher dazu, dass die Mediennutzung heimlich erfolgt und die Kinder/Jugendlichen Fragen oder belastende Erfahrungen nicht mit den Fachpersonen teilen.</p>

Hinweise zu gesetzlichen Grundlagen

Der Wert von Freiheit und Selbstbestimmung prägt die gesamte Rechtsordnung (Bundesverfassung, kantonale Verfassungen, Völkerrecht, Strafrecht, Privatrecht). Auch zum Datenschutz ist die gesetzliche Ordnung zum Datenschutz unübersichtlich, mit mehr als 150 Bundeserlassen, zusätzlich Erlassen im Strafrecht und im Zivilrecht, ausserdem bestehen sowohl bundesrechtliche als auch kantonale rechtliche Datenschutznormen.

Wichtige Gesetzesartikel:

Schweizerische Bundesverfassung

Art. 10: Recht auf persönliche Freiheit

Art. 13: Anspruch auf Schutz vor Missbrauch persönlicher Daten und auf informationelle Selbstbestimmung

Strafgesetzbuch

Insb. Art. 320 (Amtsgeheimnis)

Zivilgesetzbuch

Art. 11 -19: Rechtsfähigkeit, Handlungsfähigkeit, Urteilsfähigkeit

Art. 28: Schutz der Persönlichkeit gegen Verletzungen

Datenschutzgesetz: DSG; kantonale Datenschutzgesetze

Europäische Menschenrechtskonvention: Art 8: Recht auf Achtung des Privatlebens