

**Autor:** Liesching, Marc.

**Titel:** Datenschutz in Online-Communitys.

**Quelle:** merz. medien+erziehung. 53. Jahrgang, Heft 8/09. München 2009, S. 22-26.

**Verlag:** kopaed.

Die Veröffentlichung erfolgt mit freundlicher Genehmigung des Verlags.

---

*Marc Liesching*

# **Datenschutz in Online-Communitys.**

**Rechtlicher Rahmen und Konsequenzen für Betreiber und Nutzende.**

## **Verfassungsrechtliche Verankerung und Zielsetzung des Datenschutzrechts**

Das Datenschutzrecht umschreibt den Rechtsbereich in Bezug auf den Schutz personenbezogener Daten jedes einzelnen Bürgers und jeder Bürgerin. Es ist abgeleitet aus dem verfassungsrechtlichen Grundsatz des informationellen Selbstbestimmungsrechts, der nach der Rechtsprechung des Bundesverfassungsgerichts wiederum Teil des durch Art.2 Grundgesetz (GG) geschützten allgemeinen Persönlichkeitsrechts ist. Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz der Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe von persönlichen Daten also von dem allgemeinen Persönlichkeitsrecht des Art. 2 1 i. V. mit Art. 1. Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis der Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung ihrer persönlichen Daten zu bestimmen. In seinem grundlegenden „Volkszählungs-Urteil“ hat das Bundesverfassungsgericht klargestellt, dass Einschränkungen dieses Rechts auf „informationelle Selbstbestimmung“ nur „im überwiegenden Allgemeininteresse“ zulässig sind. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muss. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat

---

er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken. Bei den verfassungsrechtlichen Anforderungen an derartige Einschränkungen ist nach dem Bundesverfassungsgericht zu unterscheiden zwischen personenbezogenen Daten, die in individualisierter, nicht anonymer Form erhoben und verarbeitet werden und solchen, die für statistische Zwecke bestimmt sind.

Vordem Hintergrund der Vorgaben des Bundesverfassungsgerichts haben Bund und Bundesländer allgemeine Datenschutzgesetze erlassen, die durch Spezialgesetze zum Beispiel für den Sozialbereich oder etwa auch für den Bereich der sogenannten „Telemedien“ (insbesondere Internetangebote) ergänzt werden. § 1 Abs. 1 des Bundesdatenschutzgesetzes formuliert die Intention des Datenschutzrechts insoweit wie folgt: „Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird“. Dieser Leitgedanke wird durch das Bundesdatenschutzgesetz aber auch durch andere gesetzliche Regelungen weiterhin in allgemeinen datenschutzrechtlichen Grundsätzen konkretisiert, auf die nachfolgend eingegangen wird. Zuvor sollen aber die im Datenschutz maßgeblichen Begrifflichkeiten erläutert werden.

## **Begrifflichkeiten des Datenschutzrechts**

Zentraler Begriff des Datenschutzes ist zunächst das Schutzobjekt, namentlich sind das die sogenannten „personenbezogenen Daten“. Hierunter werden alle Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person (Betroffener oder Betroffene) verstanden, wobei Einzelangaben jeglicher Art erfasst werden, die insbesondere nicht auf Angaben in Dateien beschränkt sind. Beispiele für personenbezogene Daten sind etwa Vor-, Nachnamen, Postanschriften, E-Mail-Adressen, Telefonnummern, persönliche Verhältnisse (Familienstand, Hobbys usw.) oder Gewohnheiten (Raucher, Sportler usw.). Gerade nicht als personenbezogene Daten erfasst sind hingegen anonymisierte Angaben, die keiner konkreten Person mehr zugeordnet werden können.

Von besonderer Bedeutung ist weiterhin, in welcher Art und Weise mit Daten verfahren wird. Das Datenschutzrecht benennt hier insbesondere Vorgänge des Erhebens, Verarbeitens oder Nutzens von Daten. Das Erheben von Daten bezeichnet dabei das Beschaffen von Daten über einen Betroffenen oder eine Betroffene. Das Verarbeiten von Daten umfasst Vorgänge des Speicherns, Veränderns, Übermitteln und Löschns personenbezogener Daten. Schließlich umfasst als Auffangbegriff das „Nutzen von Daten“ jede Verwendung personenbezogener Daten, soweit es sich nicht um eine Verarbeitung handelt (insbesondere die Weitergabe von Daten innerhalb der speichernden Stelle an Teile derselben Stelle mit anderen Aufgaben oder anderem örtlichen Zuständigkeitsbereich).



Das Datenschutzrecht soll für Sicherheit im Umgang mit Daten sorgen.

## **Grundsätze des Datenschutzrechts**

Wichtigster Grundsatz des Datenschutzrechts ist nun, dass öffentliche oder private Stellen personenbezogene Daten von Bürgern und Bürgerinnen nicht in der gerade beschriebenen Art und Weise einfach erheben, verarbeiten oder sonst nutzen dürfen. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, wenn (1.) eine Rechtsvorschrift sie (ausdrücklich) erlaubt oder anordnet oder (2.) der Betroffene

eingewilligt hat. Das Datenschutzrecht schreibt also einen strengen Regel-Ausnahme-Mechanismus betreffend die Verwendung personenbezogener Daten vor (sog. „Verbot mit Erlaubnisvorbehalt“). Verstöße gegen den Grundsatz sind größtenteils im Rahmen von Straf- und Ordnungswidrigkeitenvorschriften sanktioniert. Die praktische Bedeutung der Verfolgung von Verstößen ist jedoch gering, wie insbesondere die jährlichen polizeilichen Kriminalstatistiken ausweisen.

Als weitere wichtige allgemeine Grundsätze finden sich im Datenschutzrecht die Axiome der Datenvermeidung und Datensparsamkeit (vgl. z. B. § 3a BDSG). Diese geben den arbeitenden öffentlichen und privaten Stellen die Zielvorgabe vor, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Freilich ist diese recht allgemeine Vorgabe ein stumpfes Schwert im Hinblick auf die tatsächliche Umsetzung des sparsamen Umgangs mit personenbezogenen Daten. Auch Datenschutzbeauftragte des Bundes und der Länder beklagen in ihren Jahresberichten regelmäßig Verstöße im Sinne eines inflationären Sammelns und Nutzens von Daten der Bürgerinnen und Bürger, die zudem unüberschaubar sind und vermutlich nur in seltenen Fällen aufgedeckt werden.

## **Spezialregelungen für die Erstellung von Nutzungsprofilen**

Die Erstellung von Nutzungsprofilen hat im Lichte der Wirtschafts- und Marketinginteressen gerade im Bereich des Internets in erheblichem Maße an praktischer Bedeutung gewonnen. Der Gesetzgeber hat hier vergleichsweise frühzeitig mit Sonderregelungen für den Bereich der Telemedien reagiert. Insbesondere nach §15Abs.3 des Telemediengesetzes (TMG) darf der Diensteanbieter für Zwecke der Werbung, der Marktforschung oder auch zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile unter Verwendung von Pseudonymen nur erstellen, sofern der Nutzende dem nicht widerspricht.

Der Diensteanbieter hat die Nutzerin bzw. den Nutzer des Weiteren auf ihr bzw. sein Widerspruchsrecht im Rahmen der allgemein bestehenden Unterrichtungspflicht hinzuweisen. Diese Nutzungsprofile dürfen nicht mit Daten über den Träger bzw. die Trägerin des Pseudonyms zusammengeführt werden. Allerdings ist zu bemerken, dass

die Einschränkungen nur für den Fall gelten, dass die betroffenen Nutzerinnen und Nutzer nicht in eine weitergehende Profilierung eingewilligt haben. Von besonderer praktischer Bedeutung - vor allem auch für die häufig von Minderjährigen genutzten Communitys und Social Networks - ist damit die Fragestellung, welche Anforderungen an Einwilligungen zu stellen sind und unter welchen Voraussetzungen auch Kinder und Jugendliche in die Verwendung ihrer personenbezogenen Daten (ohne Zustimmung der Eltern) überhaupt wirksam einwilligen können.

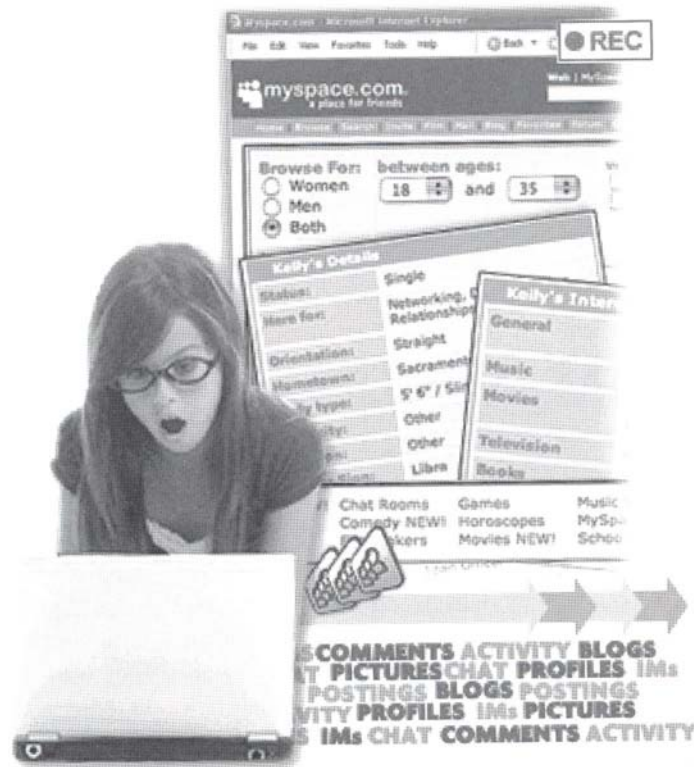
## **Anforderungen an datenschutzrechtliche Einwilligungen**

Im Zusammenhang mit der Nutzung von Online-Communitys und Social Networks kommen sowohl ausdrückliche als auch konkludent (also schlüssig) erklärte Einwilligungen in die Datennutzung in Betracht. Eine ausdrückliche Einwilligung liegt zunächst vor, wenn bereits der Wortlaut einer Erklärung einen konkret zu beurteilenden Eingriff rechtfertigt. Eine solche Einwilligungserklärung erfordert allerdings neben der Dispositionsbefugnis des Rechtsgutinhabers bzw. der Rechtsgutinhaberin und der entsprechenden Einwilligungserklärung vor allem die Einwilligungsfähigkeit der Betroffenen, das Fehlen von erheblichen Kinder können die Konsequenzen ihres Handelns im Internet oft Willensmängeln sowie die Auf- noch nicht überblicken klärung der Einwilligenden.

Eine wirksame Einwilligung setzt dabei voraus, dass die Betroffenen Bedeutung und Tragweite seiner bzw. ihrer Entscheidung überblickt. Unter diesem Gesichtspunkt problematisch sind daher vor allem pauschale und formularmäßige Ermächtigungen.

Auch konkludent erklärte Einwilligungen in die Verwendung von Daten sind grundsätzlich denkbar. Insbesondere dann, wenn Nutzende freiwillig Einzelangaben zur eigenen Person oder auch Lichtbilder auf einer Plattform im Internet veröffentlichen, kann davon ausgegangen werden, dass sie sich auch schlüssig mit deren Speicherung und Verbreitung durch den jeweiligen Plattformbetreiber einverstanden erklären. Aus Rechtssicherheitsgründen sind die großen Plattformbetreiber freilich sehr schnell dazu übergegangen, im Rahmen ihrer Nutzungsbedingungen oder allgemeinen Geschäftsbedingungen auch auf die datenschutzrechtliche Dimension hinzuweisen und

damit durch die Akzeptanz der Bedingungen durch die Nutzerinnen und Nutzer zugleich auch eine datenschutzrechtliche Einwilligung einzuholen.



© netbus.org

*Kinder können die Konsequenzen ihres Handelns im Internet oft noch nicht überblicken.*

Problematisch sind freilich die Fälle, in denen es sich um minderjährige Nutzende handelt. Hier sind die Anforderungen an eine wirksame Einwilligung in die Verwendung von personenbezogenen Daten von Kindern und Jugendlichen umstritten. Herrschende Meinung scheint insoweit allerdings zu sein, dass jedenfalls bei geschäftsunfähigen und nicht einsichtsfähigen Kindern stets die Einwilligung der personensorgeberechtigten Personen als gesetzliche Vertreter (Eltern) erforderlich ist. Bei einsichtsfähigen Kindern und Jugendlichen (in der Regel ab zwölf Jahren) wird hingegen teilweise sowohl die Einwilligung der Eltern als auch der abgebildeten Kinder bzw. Jugendlichen gefordert. Nach liberalerer und vor allem in der Praxis häufig anzutreffender Gegenauffassung

genüge bei Einsichtsfähigkeit von Kindern und Jugendlichen alleinig deren wirksame Einwilligung; zusätzliche Einwilligungen der Eltern wären danach nicht erforderlich.

Entsprechend der liberalen Rechtsauffassung finden sich bei Online-Communitys, die sich an Kinder und Jugendliche richten, auch präventive Bedingungen und Erklärungen, wie etwa die ausschließliche Ausrichtung des eigenen Internetangebotes „an Schüler und Schülerinnen ab zwölf (12) Jahren“. Anmeldungen werden zudem an die Voraussetzung bzw. Bedingung geknüpft, dass sich die Nutzerin bzw. der Nutzer „über die Konsequenzen der Erhebung, Verarbeitung und Speicherung deiner persönlichen Daten bewusst“ ist und „die Bedeutung der Datenverarbeitung und -Speicherung“ versteht, ergänzt um den Hinweis, dass dies eine „gewisse Einsichtsfähigkeit und Reife“ erfordere. Schließlich wird darauf hingewiesen, dass von einer Anmeldung zu der Internetplattform abgesehen werden müsse, wenn der oder die Nutzende „jünger als zwölf (12) Jahre“ oder „kein Schüler“ ist, oder wenn er oder sie „die Bedeutung der Erhebung, Verarbeitung und Speicherung der [...] angegebenen persönlichen Daten nicht in vollem Umfang“ versteht. Eine weitergehende Überprüfung oder Kontrolle von Daten der sich anmeldenden Nutzenden im Hinblick auf tatsächliches Alter oder Einsichtsfähigkeit findet sodann freilich nicht statt.

## **Konsequenzen für Online-Communitys und Social Networks**

Freilich kann ein überkritischer Blick auf die gerade geschilderten Gegebenheiten wiederum vordem Hintergrund hinterfragt werden, dass es den heute allgemein etablierten Social Networks nachgerade immanent ist, dass Benutzerinnen und Benutzer ihre personenbezogenen Daten einschließlich ihrer Lichtbildnisse preisgeben, um sich entsprechend zu präsentieren. Auch dies ist Ausdruck ihres verfassungsrechtlich verbürgten Selbstbestimmungsrechts einschließlich der Art und Weise der Selbstdarstellung. Als problematisch sind vor diesem Hintergrund lediglich solche Fälle anzusehen, in denen eine Nutzung der Internet-Plattformen zum Beispiel durch Kinder erfolgt, welche die Tragweite eines freigiebigen Umgangs mit personenbezogenen Daten noch nicht überblicken können. Hier wäre zu wünschen, dass künftig Gerichte oder auch der Gesetzgeber klare Grenzen setzt, aber auch Lösungsmöglichkeiten aufzeigt, welche

den tatsächlichen Gegebenheiten einer völlig üblichen und sozial etablierten Nutzung von Social Communitys Rechnung trägt. Neben den rein rechtlichen und gesetzgeberischen Möglichkeiten wird in diesem Feld vor allem aber auch der Pädagogik die Aufgabe zufallen, Kinder und Jugendliche für den sorgsam und verantwortungsbewussten Umgang mit eigenen personenbezogenen Daten zu sensibilisieren und zu schulen.

*Alle Rechte, insbesondere das Recht der Vervielfältigung und Verbreitung sowie der Übersetzung, vorbehalten. Kein Teil des Werkes darf in irgendeiner Form (durch Fotokopie, Mikrofilm oder ein anderes Verfahren) ohne schriftliche Genehmigung des Rechteinhabers reproduziert oder unter Verwendung elektronischer Systeme weiterverarbeitet, vervielfältigt oder verbreitet werden.*