Projekt Kodex für Soziale Netzwerke

Closing Report, April 2013

I. Einleitung

Seit Ende 2011 arbeitet die FSM gemeinsam mit den Unternehmen Facebook Germany GmbH, Google Germany GmbH, LinkedIn Corporation, Lokalisten Media GmbH, StayFriends GmbH, Poolworks (Germany) Ltd., wer-kennt-wen.de GmbH und XING AG an einem Kodex für Soziale Netzwerke, der die Bereiche Datenschutz, Jugendschutz und Verbraucherschutz abdecken soll. Die Initiative hierfür wurde im Sommer 2011 durch das Bundesministerium des Innern (BMI) gestartet. Dabei hat die FSM die Rolle des Moderators für die inhaltlichen Verhandlungen übernommen.

Erklärtes Ziel ist es, in diesen Bereichen zu einer Selbstregulierung zu kommen, die einen Mehrwert für den Verbraucher darstellt und – zumindest für den Bereich des Datenschutzes - einen Ausweg aus den vertrackten Diskussionen zwischen Unternehmen und insbesondere den Datenschutzaufsichtsbehörden bedeutet.

Im Hinblick auf die notwendige Einbeziehung der Landesdatenschutzbeauftragten, denen über §38a BDSG zumindest grundsätzlich ein Instrument für die Anerkennung von Selbstregulierung zur Verfügung steht, fand von Anfang an dabei der Beschluss des Düsseldorfer Kreises vom 8. Dezember 2011[1] Berücksichtigung, bei dem die Landesdatenschutzbeauftragten sich abschließend zu ihren damaligen Vorstellungen hinsichtlich zu erfassender Themen äußerten.

[1] Beschluss des Düsseldorfer Kreises abrufbar unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/08122011DSInSozialenNetzwerken.pdf?__blob=publicationFile

II. Das Instrument der Selbstregulierung

Das Konzept der Selbstregulierung ist im Bereich Datenschutz in den vergangenen Wochen und Monaten ausführlich diskutiert worden. Das BMI hat aus guten Gründen die Schaffung eines rechtlichen Rahmens für Selbstregulierung auch auf der europäischen Ebene vertreten[2]. Es sind aber auch kritische Stimmen zu diesem Ansatz laut geworden.

1. Erfahrungen aus dem Bereich des Jugendmedienschutzes

Mit diesem Bericht möchte die FSM zunächst die Möglichkeit effizienter Selbstregulierung mit Verweis auf die eigene Geschichte unterstreichen. Diese zeigt, dass Selbstregulierung bei Bestehen eines hinreichend genauen gesetzlichen Rahmens effizient und unter Einbeziehung aller Kräfte funktionieren kann. Die erfolgreiche Arbeit der Selbstregulierung im Bereich des deutschen Jugendmedienschutzes wird sowohl durch die Evaluation des Hans-Bredow-Instituts[3], als auch durch Aussagen der Politik und Aufsicht bestätigt[4].

Der Jugendmedienschutz zeigt, dass ein solches System durch einen entsprechenden regulativen Rahmen aufgesetzt werden kann. Es besteht eine gesetzliche Grundlage, die, anders als die im Bereich des Datenschutzes einschlägige, vage gesetzliche Vorgabe des §38a BDSG, eine hinreichend detaillierte Struktur für Selbstregulierung aufsetzt. Wesentliche Elemente hiervon sind in aller Kürze:

- Anreize zur Teilnahme an Selbstregulierung durch gesetzliche Privilegierung
- Kompetenzübertragung an die Selbstkontrolle in einem gewissen Rahmen
- Schaffen von Qualitätsstandards durch staatliche Anerkennung von Selbstkontrolle
- Kontrolle und Durchgriff der Exekutive bei groben Fehlentwicklungen.

Selbstkontrolle lebt damit von einer durch Kompetenzübertragung geschaffenen Freiheit, die es ihr ermöglicht, Regelungen schnell dem sich verändernden Umfeld, gerade im IT-Bereich,

---

[2] Siehe PM BMI vom 07.03.2013 unter
http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2013/03/jirat_datenschutz.html
sowie vom 28.02.2013 unter
http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2013/02/soziale-netzwerke.html.

[3] Bericht über Evaluation des Jugendmedienschutzes abrufbar unter
http://www.hans-bredow-institut.de/de/pressemitteilung/hans-bredow-institut-praesentiert-ergebnisse-evaluation-des-jugendmedienschutzes

[4] http://www.bitkom.org/de/themen/54758_44839.aspx und
http://www.kjm-online.de/de/pub/aktuelles/pressemitteilungen/pressemitteilungen_2012/pm_122012.cfm

anzupassen. Gleichzeitig muss sie von Gesetzes wegen vom Staat kontrollierbar sein, wenn gewisse Grenzen überschritten werden. Durch dieses Wechselspiel kann sich eine Dynamik ergeben, die eine sinnvolle Kontrolle und Selbstregulierung des betreffenden Bereichs zur Folge hat, ohne als bloßes Feigenblatt zu enden.

Diese Voraussetzungen haben etwa dafür gesorgt, dass die Selbstregulierung im Jugendschutz sich nicht zum „zahnlosen Tiger" entwickelt hat, sondern effektiv die Mitgliedsunternehmen überwacht und damit auch kritische Gegenstimmen überzeugt werden konnten. Nicht zuletzt gehört hierzu auch der bereits 2009 geschlossene Kodex zu Sozialen Netzwerken, dem sich deutsche Netzwerke angeschlossen haben[5]. Beispielhaft sei zudem der Kodex der deutschen Suchmaschinendienste in Kooperation mit der BPJM genannt[6]. Es kann festgestellt werden, dass im Bereich der Mitglieder von anerkannten Selbstkontrollen wie z.B. der FSM kaum noch Jugendschutzverstöße auftreten.

2. Möglichkeiten von Selbstregulierung im Bereich des Datenschutzes

Selbstregulierung ist aus Sicht der FSM auch im Datenschutz ein potentiell sinnvolles Instrument, weil die Exekutive dort – wie im fast gesamten IT-Bereich - mit einer unüberschaubaren Masse an potentiellen Verstößen und einer sehr schnellen Entwicklung der angebotenen, datenverarbeitenden Dienste zu kämpfen hat. Aufgrund dieser Dynamik ist eine effektive Aufsicht in vielen Fällen schlichtweg schwierig. Nicht zuletzt im Datenschutz lässt sich beobachten, dass auch eine faktische Kontrollierbarkeit technischer Strukturen nicht in allen Bereichen effektiv stattfinden kann.

Die jüngst immer wieder geäußerte Kritik an fehlender Effektivität und Durchschlagskraft von Selbstregulierung wird des Öfteren und so auch derzeit im Bereich des Datenschutzes als Fundamentalkritik geäußert. Die von dieser Seite angeführten Defizite sind jedoch aus Sicht der FSM durch konkrete gesetzliche Grundlagen, die einen geeigneten Rahmen für Selbstregulierung aufsetzen, vermeidbar und nicht intrinsisch dem Konzept von Selbstregulierung eigen.

Selbstkontrolle kann helfen, die Exekutive zu entlasten sowie über Kodizes schnelle und moderne Regelungen umzusetzen. Dabei sollen und müssen sich diese Regelungen an

[5] http://www.fsm.de/selbstverpflichtungen/social-communities
[6] http://www.fsm.de/selbstverpflichtungen/suchmaschinen

inhaltlichen, gesetzlichen Rahmenvorgaben messen lassen, aber sie muss auch einen Entscheidungsspielraum haben, der nicht von vornherein auf null reduziert ist. Eine anerkannte Selbstkontrolle ist keine „Polizei“ die im Rahmen enger Vorgaben und auf konkrete Anweisung tätig wird, sondern sie muss selbst agieren und regulieren können, lediglich der Rahmen hierfür muss durch den Staat kontrollierbar sein.

Im Datenschutz indes bestehen diese gesetzlichen Voraussetzungen nicht.

Der bestehende §38a BDSG sagt weder etwas über Verfahrensfragen, noch über eine Kompetenzzuweisung an die Selbstkontrolle. Damit sind Regelungen nach §38a BDSG davon abhängig, ob de-facto eine belastbare Absprache zwischen Wirtschaft und Datenschutzbehörden stattfindet, und ob diese Absprache eingehalten wird. Dies ist im Rahmen der kontroversen, inhomogenen und in der Öffentlichkeit ausgetragenen Diskussion zu Datenschutz in Sozialen Netzwerken keine einfache Aufgabe. Zudem ist es für beide Seiten mit einer erheblichen Rechtsunsicherheit verbunden. Es ist ein auf allen Seiten bestehendes Misstrauen festzustellen, sich auf ein gemeinsames, pragmatisches Vorgehen einzulassen. Eine klare Zuweisung von Kompetenzen wäre notwendig.

3. Das Zwischenergebnis der Verhandlungen als Beitrag zur Zukunft von Selbstregulierung

Vor dem beschriebenen Hintergrund einer fehlenden, hinreichend konkreten gesetzlichen Grundlage wurden die Verhandlungen der Betreiber Sozialer Netzwerke durch die Ankündigung der europäischen Datenschutzverordnung noch komplexer. Im Lichte der Ankündigung einer europäischen Regulierung, die weitestgehend deutsches Datenschutzrecht „überschreiben“ wird, musste zunächst sondiert werden, wie sich eine nun gestaltete, nationale Selbstregulierung hier einfügen kann. Während die national agierenden Unternehmen sich insbesondere mit den Vorgaben des jeweils zuständigen Landesdatenschutzbeauftragten auseinanderzusetzen hatten, waren die international agierenden Unternehmen zunächst bestrebt, Vorgaben zu erhalten, die für ganz Europa einheitlich gelten können. Damit wollte man verhindern, nun kurzfristig nationale Verpflichtungen einzugehen, ohne dass klar ist, ob und wie diese durch die Vorgaben der europäischen Datenschutzverordnung noch zur Geltung kommen können. Dies ist absolut

verständlich, da technische Änderungen bei grenzüberschreitenden Angeboten immer sehr weitreichende Auswirkungen haben.[7][8]

Vor diesem Hintergrund waren die Verhandlungen von der Frage geprägt, wie eine nationale Selbstregulierung dieser Notwendigkeit nach europäischer Harmonisierung gerecht werden und gleichzeitig die Anforderungen der Datenschützer erfüllen kann.

Dabei waren und sind die FSM und die Betreiber der Sozialen Netzwerke auf die Hilfe der Politik und der Datenschutzbehörden angewiesen. Es muss ein Konsens und eine Perspektive dahingehend geschaffen werden, dass selbstregulative Regelungen auch europäisch nutzbar sind. Dies führt zu der schwierigen Frage, inwieweit das Bundesdatenschutzgesetz, das in weiten Teilen schon bald nicht mehr einschlägig sein könnte, für diese Regelung als Maßstab dienen soll.

Die FSM und die beteiligten Unternehmen haben sich in den Verhandlungen am BDSG und den in dem Beschluss aufgeführten Vorgaben der Landesdatenschutzbeauftragten vom 8.12.2011 orientiert, dabei aber versucht, die nach wie vor diskutierten Entwürfe der europäischen Datenschutzverordnung zu berücksichtigen.

In diesem Lichte ist auch die anstehende Diskussion der nun vorgelegten Entwürfe zu einer solchen Selbstregulierung zu lesen. Die FSM und die Unternehmen demonstrieren mit diesen Überlegungen den Willen, an dieser Diskussion konstruktiv teilzunehmen. Dabei wird auch die Notwendigkeit für klare europäische Rahmenbedingungen für Selbstregulierung deutlich.

Die FSM steht bereit, die hier vorgelegten Inhalte mit den politischen Kräften und den Aufsichtsbehörden vor diesem Hintergrund zu diskutieren. Selbstregulierung, auch internationale, braucht eine effektiv arbeitende Selbstregulierungsinstitution, und auch hier bietet die FSM aufgrund ihrer langjährigen Erfahrung im Online-Bereich ihre Hilfe an. Es ist

---

[7] Die Google Germany GmbH hat den Prozess über die vergangenen Monate intensiv und aktiv begleitet. Sie glaubt an die Arbeit und Ziele, die im Rahmen des Projekts vorangetrieben werden und wird den Prozess als unterstützender Beobachter jedoch nicht mehr als potentieller Unterzeichner weiterhin begleiten. Vor dem bezeichneten Hintergrund globaler Bestrebungen, einen zunehmend supra-nationalen Regelungsansatz für Kernfragen internetbezogener Regulierung zu finden und der globalen Produktausrichtung des Unternehmens begegnet eine weitere Regelungsfragmentierung während des laufenden Harmonisierungsprozesses jedoch Bedenken. Die Google Germany GmbH nimmt daher von der Zeichnung Abstand.

[8] Die Facebook Germany GmbH, die LinkedIn Cooperation, die XING AG und die StayFriends GmbH nehmen ebenfalls von der Zeichnung Abstand.

dafür notwendig, dass Politik und Aufsicht die internationale Perspektive sowie Platz und Kompetenz von Selbstregulierung in diesem Bereich konkret aufzeigen.

III. Derzeitiger Stand der Verhandlungen

Die FSM hat daraufhin bis zum jetzigen Zeitpunkt insgesamt zwölf mehrstündige Arbeitssitzungen durchgeführt, nämlich am

25.01.2012, 22.02.2012, 03.04.2012, 03.05.2012, 31.05.2012, 28.06.2012, 23.07.2012, 24.07.2012, 21.08.2012, 25.09.2012, 19.11.2012, 10.01.2013.

Dazu kamen eine Reihe von Telefonkonferenzen, die letzte am 08. März 2013. In diesen Sitzungen haben die Unternehmen und die FSM inhaltliche Regelungen erarbeitet (siehe Punkt IV. Inhalte), die nun im Rahmen dieses Berichts als Grundlage der weiteren Diskussion angeboten werden.

Mit den hier vorgelegten Inhalten zeigen die Unternehmen und die FSM, dass Selbstkontrolle gewollt und auch in der Lage dazu ist, inhaltlich sinnvolle Vorschläge zu erarbeiten. Sie sollen als Diskussionsgrundlage für den weiteren, notwendigen Prozess dienen, der vor allem eine konkrete Perspektive für die Umsetzung von Selbstregulierung im europäischen Rahmen schaffen muss. Hierzu müssen ganz konkrete Voraussetzungen mit Hilfe gesetzlicher Vorschriften geschaffen werden.

1. Inhaltliche Fokussierung auf den Datenschutz und die Punkte des Düsseldorfer Kreises

Themen des angestrebten Kodex sind neben Datenschutz auch Jugend- und Verbraucherschutz. Aufgrund der im Vorfeld formulierten Anforderungen der beteiligten politischen und exekutiven Kräfte hat die FSM sich gemeinsam mit den Unternehmen zunächst auf den Bereich des Datenschutzes fokussiert.

Dabei hat man sich auf die im Beschluss vom 8.12.2011 durch den Düsseldorfer Kreis genannten Punkte[9] konzentriert.

Noch offene Punkte sind der Jugendschutz und der Verbraucherschutz. Gerade die datenschutzrechtlichen Besonderheiten bei Kindern und Jugendlichen, die aus Sicht der FSM

[9] Beschluss des Düsseldorfer Kreises abrufbar unter
http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/08122011DSInSozialenNetzwerken.pdf?__blob=publicationFile

aufgrund der besonderen Schutzwürdigkeit dieser Gruppe besondere Aufmerksamkeit verdienen, wurden aufgrund des bisher allgemein gewünschten Schwerpunktes auf den Datenschutz noch nicht behandelt. Die Arbeit an diesen Punkten soll schnellstmöglich beginnen.

2. Veröffentlichung zum jetzigen Zeitpunkt als Closing Report

Aufgrund der gesetzlichen und politischen Situation in Deutschland und der erwähnten europäischen Entwicklungen im Bereich des Datenschutzes hält es die FSM für zielführend, die bisher erzielten Ergebnisse im Datenschutz in dieser Form zum jetzigen Zeitpunkt zu veröffentlichen, damit diese in die laufende Debatte einfließen können.

Gleichzeitig benötigen die weiteren Verhandlungen für ein Fortkommen eine konkrete Perspektive dafür, wie ein europäischer Rechtsrahmen für Selbstregulierung unter Einbeziehung der deutschen Datenschutzbehörden aussehen kann und welche Standards durch die europäische Ebene gesetzt werden sollen. Die FSM und die beteiligten Unternehmen stellen in diesem Sinne die bisher erzielten Ergebnisse als Diskussionsgrundlage vor dem oben beschriebenen Hintergrund zur Verfügung.

_____

Ralf Bartoleit, Lokalisten Media GmbH

_____

Joseph Nejman, poolworks (Germany) Ltd

ppa.

Mirko Meurer, wer-kennt-wen.de GmbH

IV. Inhalte

Entwurf:

Verhaltenskodex für Anbieter sozialer Netzwerke

Erarbeitete Regelungen, Arbeitsstand: 13.03.2013

Begriffsbestimmungen

Folgende Definitionen bezeichnen innerhalb dieses Verhaltenskodex bezeichnete Begriffe.

- Soziale Netzwerke sind Webportale, die ihren Nutzern üblicherweise folgende Funktionen anbieten:
  - Erstellung eines persönlichen Profils
  - Kontaktliste oder Adressbuch
  - Empfang und Versand von Nachrichten an andere Mitglieder
  - Empfang und Versand von Benachrichtigungen über bestimmte Ereignisse
  - Veröffentlichen von Statusaktualisierungen
  - Austausch der Nutzer über gemeinsame Interessen.

  In der Regel ist der Hauptzweck eines Netzwerkes die Kommunikation und Kontaktpflege der Nutzer untereinander.[10]
- Anbieter sind die Betreiber eines sozialen Netzwerks, die diesen Verhaltenskodex unterzeichnen.
- Nutzer sind in Deutschland ansässige, natürliche Personen, die sich für die Nutzung von Diensten der Anbieter registriert haben. Soweit der Nutzer in einer vom Anbieter dafür vorgesehenen Weise seinen Aufenthaltsort angibt, ist diese Angabe ausschlaggebend.[11]
- Dienst ist das soziale Netzwerk als telemediales Angebot.
- Altersangaben beziehen sich auf das vom Nutzer in der vom Anbieter dafür vorgesehenen Weise angegebene Alter.
- Unter Gesichtserkennung versteht man die Identifizierungsmöglichkeit einer Person mittels biometrischer Gesichtserkennungsmerkmale.
- Berufliche Netzwerke sind Dienste, deren selbstbestimmter Hauptzweck es ist, berufliche bzw. geschäftliche Kontakte bzw. Aktivitäten der Nutzer zu fördern.

---

[10] Eine Definition des Begriffes „Soziale Netzwerke“ schien den Unterzeichnern erforderlich, da der Kodex auf diese Art von Diensten beschränkt sein soll. Auf Grund ständig neu entstehender Diensteformen im Internet und der Verschmelzung unterschiedlicher Dienste, wurde hier insbesondere der Hauptzweck der Kommunikation und Kontaktpflege in den Vordergrund gestellt.

[11] Die Definition des Nutzers dient der lokalen Begrenzung des Kodexes auf in Deutschland ansässige Personen.

Schutz von Nichtnutzern im Rahmen des Adressbuchabgleich

Ziel der Regelung ist es, die Nutzer umfassend über die Funktionsweise des Adressbuchabgleichs zu informieren sowie die Daten Dritter (=Nichtnutzer) zu schützen.

(1) Unter einem Adressbuchabgleich versteht man das Hochladen von Adressdaten in den Dienst eines Anbieters, um dem Nutzer das Auffinden von anderen, ihm bekannten Nutzern des Dienstes zu ermöglichen. Diese Funktion kann auch zur Kontaktaufnahme mit Personen dienen, die noch nicht Nutzer des Dienstes sind.

(2) Der Nutzer wählt aktiv aus, dass ein Adressbuchabgleich (je nach Ausgestaltung des Dienstes: einmalig oder automatisiert wiederholt) erfolgen soll und welchen Personen, die noch nicht Nutzer sind, er eine Einladung zur Registrierung des Dienstes schicken möchte. Der Anbieter verschickt ohne entsprechende Entscheidung des Nutzers keine Einladungen. Die Einladungen enthalten einen Hinweis darauf, warum der Adressat sie erhält. Des Weiteren enthält die Einladung Informationen darüber, wie man künftige Einladungen zu diesem Dienst an die bei der Einladung verwendete Empfängeradresse verhindern kann. Der Anbieter darf die für den Vorgang des Adressbuchabgleichs vom Nutzer eingegebenen Zugangsdaten zu einem Drittdienst nicht länger als erforderlich speichern, soweit keine Einwilligung des Nutzers vorliegt.

(3) Sofern der Anbieter einen automatisierten wiederholten Adressbuchabgleich anbietet, ist der Nutzer vor der Aktivierung ausführlich auf die Funktionsweise des automatisierten Adressbuchabgleichs hinzuweisen. Der Nutzer muss diesen Vorgang jederzeit beenden können. Soweit der automatisierte Adressbuchabgleich für einen Nutzer aktiviert ist, muss in den Privatsphäre-Einstellungen deutlich für den Nutzer erkennbar sein, dass diese Funktion aktiviert ist.

(4) Der Anbieter ermöglicht dem Nutzer, alle bei der Nutzung dieser Funktion hochgeladenen und für diesen Nutzer gespeicherten Daten Dritter wieder zu löschen.

(5) Nutzer müssen im Vorfeld an prominenter Stelle über die Funktionsweise des Adressbuchabgleichs umfassend und leicht verständlich aufgeklärt werden. Dabei werden sie auch darauf hingewiesen, dass persönliche Daten Anderer durch den Datenimport an den Anbieter übermittelt werden.

Privatsphäre-Einstellungen

Ziel dieser Regelung ist es, die Nutzer umfassend zu informieren, damit sie Privatsphäre-Einstellungen bewusst und selbstbestimmt vornehmen können.

(1) Der Anbieter schafft für den Nutzer die fortlaufende Möglichkeit, seine Privatsphäre-Einstellungen während der Zeit, in der er für die Nutzung des Dienstes registriert ist, zu ändern. Es müssen nicht immer alle Einstellungsmöglichkeiten über mobile Apps / Wap-Seiten erreichbar sein, sofern alternativ auch die volle Online-Version des Dienstes über mobile Geräte erreichbar ist.[12]

(2) Der Anbieter weist die Nutzer im Rahmen des Registrierungsvorgangs, unmittelbar nach dem Registrierungsprozess oder unmittelbar nach dem ersten Login auf die Privatsphäre-Einstellungen und die Möglichkeit, diese zu ändern, deutlich hin. Ein Hinweis auf die jeweilige

[12] Um mobile Applikationen nicht zu überfrachten, ist es ausreichend, wenn alle Einstellungsmöglichkeiten in der Online-Version, die auch von mobilen Geräten aus erreicht werden kann, abrufbar sind.

Einstellungsmöglichkeit kann auch dann erfolgen, wenn die der jeweiligen Einstellungsmöglichkeit entsprechende Funktion erstmalig genutzt wird.

(3) Der Anbieter informiert die Nutzer zu Beginn des Nutzungsvorganges über die Sichtbarkeit der vom Nutzer eingestellten Inhalte im Internet sowie über die Möglichkeiten des Nutzers, mittels Einstellungsmöglichkeiten innerhalb des Dienstes diese Sichtbarkeit zu steuern. Die Information ist in allgemein verständlicher Form und gut erreichbar zu vermitteln.

(4) Die bestehenden Privatsphäre-Einstellungen eines Nutzerprofils sind auch bei einer künftigen Überarbeitung des Dienstes bzw. bei Änderungen der Voreinstellungen durch den Anbieter sowohl für bisherige als auch zukünftige Inhalte des Nutzers grundsätzlich beizubehalten. Soweit die Beibehaltung aufgrund der Umgestaltung des Dienstes technisch unmöglich oder für den Anbieter unzumutbar wird (z.B. durch Umgestaltung/ Abschaltung von Funktionen), wird der Nutzer rechtzeitig vorher darüber informiert.

Auskunfts- und Berichtigungsrechte

Ziel ist es, dem Nutzer eine nutzerfreundliche Möglichkeit zur Verfügung zu stellen, Auskunft und Berichtigung bezüglich der im Dienst über den Nutzer gespeicherten Daten zu erlangen.

(1) Der Nutzer kann vom Anbieter Auskunft verlangen über

- die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
- den Empfänger oder die Kategorien von Empfängern, an die Daten weitergegeben werden, und
- den Zweck der Speicherung.

Der Anbieter kann für die begehrte Auskunft ein automatisiertes digitales Verfahren ohne Medienbruch anbieten.

(2) Das Selbstauskunftsrecht von Kindern und Jugendlichen einerseits und die sich aus dem Fürsorgerecht ergebenen Rechte des gesetzlichen Vertreters andererseits sind von dem Anbieter zu beachten und im Einzelfall unter Abwägung aller Aspekte in Einklang zu bringen.

(3) Der Nutzer kann vom Anbieter die Berichtigung der vom Anbieter gespeicherten unrichtigen personenbezogenen Daten im eigenen Profil verlangen.

Der Anbieter kann stattdessen dem Nutzer die Möglichkeit zur Verfügung stellen, die Berichtigung der vom Anbieter gespeicherten unrichtigen personenbezogenen Daten im eigenen Profil selbst vorzunehmen.

(4) Der Anbieter stellt dem Nutzer für Auskunft und Berichtigung an leicht auffindbarer Stelle Kontaktmöglichkeiten bzw. Abruf- und Änderungsmöglichkeiten zur Verfügung.

Beendigung der Mitgliedschaft, Löschen von Daten

Ziel ist die nutzerfreundliche Möglichkeit der Beendigung der Mitgliedschaft und der Löschung von durch den Anbieter bezüglich des Nutzers im Dienst gespeicherten Daten.

(1) Der Nutzer hat jederzeit die Möglichkeit, die Nutzung des Dienstes zu beenden.

Nach Beendigung der Mitgliedschaft in einem Dienst löscht der Anbieter vorbehaltlich gesetzlicher Erlaubnistatbestände unverzüglich die vom Nutzer in den Dienst eingestellten personenbezogenen Daten.

Daten, die zur weiteren Durchführung des Vertrags nötig sind, bleiben hiervon unberührt.

(2) Sperren ist das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung durch den Anbieter einzuschränken. Die Sperrung tritt an die Stelle der Löschung, wenn eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist. Gesperrte Daten werden nicht mehr genutzt, es sei denn eine gesetzliche Erlaubnis hierfür liegt vor.

(3) Der Anbieter stellt eine einfach auffindbare Möglichkeit zur Verfügung, mit der die Beendigung auf elektronischem Wege (z.B. Button, Formular, E-Mail-Kontakt etc.) erklärt werden kann. Einfach auffindbar ist die Funktion zum Beispiel in den Einstellungen zum Konto.

(4) Der Anbieter kann aus Servicegründen eine Reaktivierung des beendeten Nutzungsverhältnisses innerhalb einer Frist von vierzehn Tagen anbieten. Dadurch werden die personenbezogenen Daten des Nutzers ab Beendigung des Nutzungsverhältnisses bis zum Reaktivierungswunsch für eine weitere Verarbeitung oder Nutzung gesperrt. Die Reaktivierungsfunktion soll dem Nutzer ermöglichen, seinen Account wiederherzustellen. Ein Anspruch des Nutzers hierauf besteht nicht.

(5) Inhalte, die vom Nutzer dem Dienst hinzugefügt (hochgeladen) wurden (z.B. Fotos, Videos, Audiodateien oder Texte) und die in Verbindung mit seinem Profil stehen, werden im Falle der Beendigung des Nutzungsverhältnisses vorbehaltlich eines abweichenden Wunsches des Nutzers oder entgegenstehender Rechtsgründe zusammen mit dem Profil entsprechend Absatz 1 gelöscht oder gesperrt. Abweichend davon können nutzergenerierte Inhalte, die im Zusammenhang mit nutzergenerierten Inhalten anderer stehen, stattdessen im Hinblick auf die automatisch vom Dienst vorgenommene Zuordnung zum Nutzer pseudonymisiert werden.[13]

Von einer Löschung, Sperrung oder Pseudonymisierung kann für bestimmte Datenkategorien im Einzelfall abgesehen werden, wenn eine Abwägung der Interessen von Nutzer, Anbieter und Dritten dem entgegensteht.[14] Ist die Speicherung von Daten nach Beendigung des Nutzungsverhältnisses aus

---

[13] Unter der Pseudonymisierung innerhalb des Kodex verstehen die Unterzeichner die Ersetzung des Namens und andere Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren. Von dieser Regelung betroffen sind hier insbesondere Beiträge in Diskussionen/Gruppen. Würden diese Kommentare gelöscht werden, so wäre in einigen Fällen der Verlauf und somit der Sinn der Diskussionen nicht mehr erkennbar.

[14] Hierunter versteht man insbesondere den Fall der Referenzen in beruflichen Netzwerken, die ein Nutzer einem anderen schreiben und dieser sodann auf seinem Profil veröffentlichen kann. Meldet sich der Aussteller der Empfehlung von dem Dienst ab, so würde die Abwägung ergeben, dass das Interesse des die Referenz empfangenen Nutzers hier einer Löschung entgegensteht, da sie Teil seines Profils geworden ist.

Rechtsgründen erforderlich oder sind Daten nicht löschbar, so wird der Anbieter in allgemeiner Form hierüber informieren.[15]

(6) Bietet ein Anbieter das zeitweise Deaktivieren eines Nutzerkontos an, informiert er den Nutzer verständlich über die Unterschiede zwischen Deaktivieren und Löschen des Nutzerkontos.

Datenschutzerklärung/ Registrierung

Ziel: Umfangreiche Unterrichtung der Nutzer im Rahmen von Datenschutzerklärungen und eine transparente Kennzeichnung von freiwilligen Angaben / Pflichtangaben im Rahmen der Registrierung.

(1) Der Anbieter unterrichtet die Nutzer im Rahmen der Registrierung darüber, welche personenbezogenen Daten erhoben und verwendet werden und zu welchem Zweck dies geschieht. Weiterhin werden die Nutzer darüber unterrichtet, an welche Empfänger bzw. an welche Kategorien von Empfängern und zu welchem Zweck diese Daten ggf. übermittelt werden.

(2) Der Anbieter stellt eine leicht zugängliche und allgemein verständliche Datenschutzerklärung zur Verfügung. Er weist die Nutzer im Rahmen der Registrierung deutlich auf die Datenschutzerklärung hin und lässt sich die Kenntnisnahme durch den Nutzer bestätigen, beispielsweise durch Anklicken eines Kästchens. Der Anbieter hält die Datenschutzerklärung auch nach der Registrierung und für Dritte jederzeit abrufbar.

(3) Aus Transparenzgründen erfolgt bereits bei der Registrierung, sofern einschlägig, eine Kennzeichnung von Pflicht- und freiwilligen Angaben des Nutzers.

Transparenz

Ziel: Stärkung der Nutzer durch transparente Informationen

(1) Der Anbieter stellt dauerhaft eine leicht zugängliche und allgemein verständliche Datenschutzerklärung auch nach der Registrierung zur Verfügung. Diesbezügliche Einzelheiten finden sich im § Datenschutzerklärung / Registrierung.

(2) Die Kontaktmöglichkeiten für den Nutzer für Auskunft und Berichtigung bzw. die diesbezüglichen Abruf- und Änderungsmöglichkeiten werden vom Anbieter an leicht auffindbarer Stelle zur Verfügung gestellt. Diesbezügliche Einzelheiten finden sich im § Auskunfts- und Berichtigungsrechte.

(3) Der Anbieter stellt nutzerfreundliche Online-Hilfen in Form von Hilfetexten/-seiten zur Verfügung.

(4) Alle aktuellen Privatsphäre-Einstellungen des Kontos des Nutzers sind für den Nutzer leicht erreichbar und in übersichtlicher Form transparent einsehbar vorzuhalten.

---

[15] Unter den hier genannten Rechtsgründen versteht man insbesondere Fälle der Strafverfolgung. In diesen Fällen ist die Information, dass bei Vorliegen von Rechtsgründen die Daten nicht gelöscht werden, in allgemeiner Form ausreichend. Dies bedeutet, dass der Anbieter bereits mit einer allgemeinen Information in den AGB/Nutzungsbedingungen diese Pflicht erfüllt. Gegen eine konkrete Information, wenn der Fall eintritt, spricht, dass man im Falle von verwirklichten Straftaten den Täter noch warnen würde.

(5) Die Anbieter bemühen sich, die Benutzeroberfläche der Dienste derart zu gestalten, dass Nutzern leicht erkennbar ist, an welchen Adressatenkreis Einladungen, Nachrichten u.ä. Kommunikationsfunktionen gerichtet sind.

(6) Der Anbieter stellt eine leicht einfach auffindbare Möglichkeit der Beendigung des Dienstes auf elektronischem Wege zur Verfügung. Diesbezügliche Einzelheiten finden sich im § Beendigung der Mitgliedschaft.

Kontaktdaten

Ziel: Leichte Möglichkeit des Kontaktes zum Anbieter

(1) An geeigneter leicht auffindbarer Stelle (z.B. im Impressum der Website) finden sich Informationen über den Anbieter sowie Verweise auf direkte Kontaktwege zur Nutzerbetreuung (z.B. E-Mail-Adresse, Formular, Hotline). Für Nutzer und Dritte muss leicht erkennbar sein, wie sie den Anbieter bzw. die Nutzerbetreuung kontaktieren und den Dienst betreffende Beschwerden abgeben können.

(2) Der Anbieter stellt mindestens eine für den Nutzer kostenfreie Möglichkeit zur Kontaktaufnahme zur Verfügung.

Gesichtserkennung

Ziel: Ermöglichung der Verwendung von biometrischen Gesichtserkennungsmerkmalen nach Einwilligung durch Nutzer

Die Verwertung von Bildmaterial (Fotos und Videos) für Zwecke der Gesichtserkennung und das Speichern und Verwenden von biometrischen Gesichtserkennungsmerkmalen sind ohne vorherige ausdrückliche Einwilligung der abgebildeten Person unzulässig. Eine solche Einwilligung liegt insbesondere vor, wenn der Nutzer bewusst und eindeutig von einer Einstellungsmöglichkeit Gebrauch gemacht hat.

Nutzungsprofile

Ziel: Information über die Erstellung von unterschiedlichen Nutzungsprofilen

(1) Unter einem Nutzungsprofil im Rahmen dieser Selbstverpflichtung versteht man die nicht vom Nutzer gesteuerte und nicht ersichtliche Erstellung personenbezogener Interessenprofile anhand von Nutzungsdaten durch den Anbieter. Die Erstellung eines Nutzungsprofils zu anderen Zwecken als zur Bereitstellung von personalisierten Funktionen des Dienstes ist nur mit Einwilligung des Nutzers zulässig.

(2) Zum Zwecke von Werbung, Marktforschung und bedarfsgerechter Gestaltung des Dienstes darf der Anbieter Nutzungsprofile unter Verwendung von Pseudonymen auch ohne Einwilligung erstellen, sofern der Nutzer dem nicht widerspricht. Der Anbieter weist den Nutzer zu Beginn des Nutzungsvorgangs auf das Widerspruchsrecht hin. Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.

Social Plugins

Ziel: Informieren des Nutzers hinsichtlich der Funktionsweise

(1) Social Plugins sind vom Anbieter bereitgestellte Funktionalitäten die durch Dritte auf ihren Websites eingebunden werden können, mittels derer die Verbindung zum Dienst hergestellt wird und der Nutzer beispielsweise signalisieren kann, dass er einen Inhalt auf dieser Website des Dritten für interessant hält.

(2) Anbieter klären die Nutzer über die Funktionsweise von Social Plugins auf. Insbesondere benennen sie die Daten, die durch die Plugins verwendet werden.

(3) Anbieter stellen die Informationen zur Verfügung, mit denen Dritte den Besuchern ihrer Websites die Funktionsweise der Social Plugins erläutern können.

(4) Sofern der Anbieter personenbezogene Daten von Nichtnutzern durch Social Plugins erhält, werden diese in der Regel innerhalb eines Monats anonymisiert.

Infrastruktur und Sicherheitsmanagement

Ziel: Einhalten eines angemessenen technischen und organisatorischen Sicherheitsniveaus

(1) Die Anbieter treffen unter Berücksichtigung des Stands der Technik technische und organisatorische Maßnahmen, die geeignet sind, ein Schutzniveau zu gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist. Insbesondere werden Maßnahmen zur Verhinderung ungewollter Datenabflüsse ergriffen.

(2) Es ist wünschenswert, dass die Anbieter Sicherheitsinfrastruktur und -management durch unabhängige Institutionen zertifizieren lassen.

Im Inland ansässiger Ansprechpartner

Ziel: Ansprechpartner für Datenschutzbehörde benennen

Die Anbieter benennen jeweils einen im Inland ansässigen Ansprechpartner für die Datenschutz-Aufsichtsbehörden.