ARTIKEL- 29 - DATENSCHUTZGRUPPE

01189/09/DE
WP 163

Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke

Angenommen am 12. Juni 2009

Inhalt

Zusammenfassung 3
1. Einführung 4
2. Definition für „soziale Netzwerkdienste (SNS)“ und Geschäftsmodell 5
3. Anwendung der Datenschutzrichtlinie 5
3.1 Wer ist der für die Datenverarbeitung Verantwortliche? 6
3.2 Sicherheits- und datenschutzfreundliche Standardeinstellungen 8
3.3 Informationspflichten des sozialen Netzwerkdienstes (SNS) 8
3.4 Sensible Daten 9
3.5 Verarbeitung von Daten von Nichtmitgliedern 9
3.6 Zugriffsmöglichkeiten durch Dritte 10
3.7 Rechtsgrundlagen für die Direktwerbung 11
3.8 Vorratsspeicherung von Daten 12
3.9 Rechte der Nutzer 13
4. Kinder und Minderjährige 14
5. Zusammenfassung der Rechte und Pflichten 15

Zusammenfassung

Diese Stellungnahme stellt auf die Frage ab, wie das Betreiben sozialer Vernetzungs-Websites mit den Bestimmungen des Datenschutzrechts der EU in Einklang zu bringen ist. Sie soll vor allem den Anbietern sozialer Netzwerkdienste (SNS) eine Richtschnur zu den Maßnahmen bieten, die zwecks der Vereinbarkeit mit dem EU-Recht verwirklicht sein müssen.

Die Stellungnahme hält fest, dass es sich bei den Anbietern sozialer Netzwerkdienste und in vielen Fällen auch bei den Drittanbietern von Anwendungs- und Softwaredienstleistungen um „für die Datenverarbeitung Verantwortliche“ mit entsprechenden Verpflichtungen gegenüber den Nutzern sozialer Netzwerkdienste handelt. Die Stellungnahme macht klar, dass sich viele Nutzer in einem rein persönlichen Lebensbereich bewegen, indem sie im Rahmen der Besorgung ihrer persönlichen oder familiären Angelegenheiten bzw. ihrer privaten Haushaltsführung Kontakte zu anderen Menschen knüpfen und unterhalten. In diesen Fällen ist nach der Stellungnahme davon auszugehen, dass die „Ausnahmeklausel für Privathaushalte betreffend persönliche oder familiäre Tätigkeiten natürlicher Personen“ Anwendung findet und die Vorschriften für die „für die Verarbeitung Verantwortlichen“ somit nicht gelten. Die Stellungnahme führt auch Umstände auf, unter denen die Tätigkeiten eines Nutzers eines sozialen Netzwerkdienstes nicht unter die „Ausnahmeklausel für Privathaushalte“ fallen. Die Verbreitung und die Verwendung von Informationen, die über soziale Netzwerkdienste verfügbar sind, zu anderweitigen, sekundären und unbefugten Zwecken gehört zu den besorgniserregenden Sicherheitsbedenken der Artikel-29-Datenschutzgruppe. Die Gruppe tritt in ihrer Stellungnahme daher für robuste sicherheits- und datenschutzfreundliche Standardeinstellungen als idealem Ausgangspunkt für alle angebotenen Dienstleistungen ein. Im Mittelpunkt der wachsenden Besorgnis stehen die Zugriffsmöglichkeiten auf Informationen aus Nutzerprofilen. Ebenso behandelt werden Themen wie die Verarbeitung sensibler Daten und Bildmaterialien, die zielgerichtete Werbung und die Direktwerbung über soziale Netzwerkdienste und die Probleme im Zusammenhang mit der Vorratsspeicherung von Daten.

Die Empfehlungen stellen im Kern auf die Verpflichtungen der Anbieter von sozialen Netzwerkdiensten ab, im Einklang mit den Vorschriften der Datenschutzrichtlinie zu handeln und die Rechte der Nutzer aufrechtzuerhalten und zu stärken. Von ganz entscheidender Bedeutung ist, dass die Anbieter von sozialen Netzwerkdiensten ihre Nutzer von Anfang an über ihre Identität aufklären und die gesamte Bandbreite der unterschiedlichen Vorhaben und Zielsetzungen darstellen, die sie mit ihrer Verarbeitung personenbezogener Daten verbinden. Besondere Sorgfalt sollten die Anbieter von sozialen Netzwerkdiensten bei der Verarbeitung personenbezogener Daten von Minderjährigen walten lassen. Die Stellungnahme empfiehlt allen Nutzern, Bilder bzw. Informationen über andere Personen nur mit der konkreten Einwilligung der jeweils betroffenen Person in ein soziales Netzwerksystem hochzuladen, und gibt auch den Anbietern von sozialen Netzwerkdiensten zu bedenken, dass sie in der Pflicht sind, ihre Nutzer im Hinblick auf die Rechte der anderen auf Schutz ihrer Privatsphäre aufzuklären.

DIE ARBEITSGRUPPE FÜR DEN SCHUTZ NATÜRLICHER PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN -

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995[1],

gestützt auf Artikel 29 sowie Artikel 30 Absatz 1 Buchstabe a) und Absatz 3 der Richtlinie, sowie auf Artikel 15 Absatz 3 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002

gestützt auf Artikel 255 EG-Vertrag und auf die Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission,

gestützt auf ihre Geschäftsordnung -

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. Einleitung

Bei der Entwicklung der Netzgemeinschaften und Webdienste, die durch Web-Anwendungen beherbergt werden, wie den sozialen Netzwerkdiensten ("SNS"), handelt es sich um ein relativ neues Phänomen, wobei die Zahl der Nutzer dieser Websites ständig exponentiell zunimmt.

Die persönlichen Informationen, die ein Nutzer dabei online bekannt gibt, in Verbindung mit den Daten, die seine Tätigkeiten und Interaktionen mit anderen Menschen nachzeichnen, können ein reichhaltiges Persönlichkeitsprofil von den Aktivitäten und Interessen dieser Person entstehen lassen. Die auf den Webportalen sozialer Netzwerke veröffentlichten personenbezogenen Daten lassen sich von unbefugten Dritten für sehr vielfältige Vorhaben und Zielsetzungen ausnutzen, so auch für kommerzielle Zwecke, und bergen in sich mitunter größere Gefahren und Risiken, wie z. B. Identitätsdiebstahl, finanzielle Einbußen, Nachteile für Geschäfts- oder Erwerbsmöglichkeiten und Beeinträchtigung der körperlichen Unversehrtheit.

Die Berliner "International Working Group on Data Protection in Telecommunications" (Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation) hat im März 2008 das *„Rom-Memorandum“*[2] verabschiedet, in dem sie die durch die sozialen Netzwerke entstandenen Risiken für die Privatsphäre und die Sicherheit analysiert und Empfehlungen für Gesetzgeber, Anbieter und Nutzer gibt. Auch die jüngst angenommene Entschließung zum Datenschutz in sozialen Netzwerkdiensten[3] stellt auf die mit diesen Diensten (SNS) einhergehenden Herausforderungen ab. Die Arbeitsgruppe berücksichtigt auch das von der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) im Oktober 2007 veröffentlichte Positionspapier “*Security Issues and Recommendations for Online Social Networks*”[4] *(Sicherheitsfragen und Empfehlungen für Soziale Online-Netzwerke),* das sich an Gesetzgeber, Anbieter und Nutzer sozialer Netzwerke richtet.

---

1 ABl. L 281 vom 23.11.1995, S. 31, http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

2 http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf

3 Angenommen auf der 30. Internationalen Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre in Straßburg am 17. Oktober 2008, http://www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_social_networks_de.pdf

4 http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

2. Definition für „soziale Netzwerkdienste (SNS)“ und Geschäftsmodell

Soziale Netzwerkdienste definiert man gemeinhin als Kommunikationsplattformen im Online-Bereich, die es dem Einzelnen ermöglichen, sich Netzwerken von gleich gesinnten Nutzern anzuschließen bzw. solche zu schaffen. Im rechtlichen Sinne handelt es sich bei den sozialen Netzwerken um Dienstleistungen der Informationsgesellschaft im Sinne des Artikels 1 Nr. 2 der Richtlinie 98/34/EG in der durch die Richtlinie 98/48/EG geänderten Fassung. Allen sozialen Netzwerkdiensten sind bestimmte Merkmale gemein:

- die Nutzer werden aufgefordert, personenbezogene Daten zur Erstellung einer Beschreibung von sich selbst bzw. eines selbst generierten persönlichen ‘Profils’ anzugeben;

- soziale Netzwerkdienste bieten auch Funktionen an, mit denen die Nutzer ihr eigenes Material (selbst generierte Inhalte wie z. B. Bilder oder Tagebucheinträge, Musik- und Videoclips oder Links zu anderen Websites[5]) dort veröffentlichen können;

- die Nutzung der sozialen Netzwerke erfolgt über die jedem Nutzer bereitgestellten Funktionen samt Kontaktliste bzw. Adressbuch, mittels derer die Verweise auf die anderen Mitglieder der Netzgemeinschaft verwaltet und zu Interaktionen mit diesen genutzt werden können.

Soziale Netzwerkdienste erwirtschaften einen Großteil ihrer Einnahmen aus der Werbung, die auf den eingerichteten Webseiten eingeblendet und von den Nutzern aufgerufen wird. Nutzer, die im Rahmen der persönlichen Profildaten große Informationsmengen über ihre Interessen veröffentlichen, bieten einen spezifisch bereinigten und fein abgestimmten Markt für Werbende, die auf der Grundlage dieser Informationen zielgerichtete Werbemaßnahmen ergreifen wollen.

Es ist daher wichtig, dass soziale Netzwerkdienste so funktionieren, dass die Rechte und Freiheiten der Nutzer beachtet werden, da diese die legitime Erwartung haben, dass die von ihnen offengelegten personenbezogenen Daten im Einklang mit dem europäischen und dem einzelstaatlichen Datenschutzrecht sowie der einschlägigen Gesetzgebung zum Schutz der Privatsphäre verarbeitet werden.

3. Anwendung der Datenschutzrichtlinie

Die Bestimmungen der Datenschutzrichtlinie gelten in den meisten Fällen auch für die Anbieter von sozialen Netzwerkdiensten, und zwar sogar dann, wenn ihr Hauptsitz außerhalb des EWR liegt. Für weitere Leitlinien zu der Frage, inwieweit die Datenschutzrichtlinie und die aufgrund der Verarbeitung von IP-Adressen und der Verwendung von Cookies zum Tragen kommenden Rechtsvorschriften auf die Einrichtung und Nutzung solcher Funktionen Anwendung finden, verweist die Artikel-29-Datenschutzgruppe auf ihre frühere Stellungnahme zu Datenschutzfragen im Zusammenhang mit Suchmaschinen.[6]

---

[5] Wenn der SNS auch elektronische Kommunikationsdienstleistungen bereitstellt, finden die Bestimmungen der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) Anwendung.

[6] WP148, „Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen“.

3.1 Wer ist der „für die Datenverarbeitung Verantwortliche“?

Anbieter sozialer Netzwerkdienste (SNS)

Die Anbieter sozialer Netzwerkdienste sind die „für die Verarbeitung von Benutzerdaten Verantwortlichen“ im Sinne der Datenschutzrichtlinie. Denn sie stellen die Mittel für die Verarbeitung der Benutzerdaten und alle „Basisdienste“ für die Benutzerverwaltung (z. B. Registrierung und Löschung von Profil- und Verkehrsdaten) bereit. Sie bestimmen auch Art und Umfang der etwaigen Nutzung der Benutzerdaten zu Werbe- und Vermarktungszwecken – so auch durch dritte Werbeanbieter.

Anbieter von Anwendungs-/Softwaredienstleistungen

Auch Softwaredienstleister/Anwendungsanbieter können „für die Verarbeitung von Benutzerdaten Verantwortliche“ sein, wenn sie Anwendungen entwickeln, die zusätzlich zu denen der sozialen Netzwerkdienste laufen und Nutzer sich zur Verwendung der betreffenden Anwendung entscheiden.

Nutzer

In den meisten Fällen sind die Nutzer als „betroffene Personen“ anzusehen. Die Pflichten des „für die Verarbeitung Verantwortlichen“ finden nach der Datenschutzrichtlinie keine Anwendung auf die Verarbeitung personenbezogener Daten, die von einer natürlichen Person *„zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten“* vorgenommen wird – sog. „Ausnahmeklausel für Privathaushalte“. Unter gewissen Umständen fallen die Tätigkeiten eines Nutzers eines sozialen Netzwerkdienstes nicht unter die „Ausnahmeklausel für Privathaushalte“, wobei dann vom Nutzer zu vermuten ist, dass er gewisse Pflichten des „für die Verarbeitung Verantwortlichen“ übernommen hat. Einige dieser Fälle werden weiter unten dargestellt:

3.1.1. Art und Zweck des sozialen Netzwerkdienstes (SNS)

Bei den sozialen Netzwerkdiensten gibt es einen zunehmenden Trend zum *„Übergang von der "Nutzung von Web 2.0 zum Vergnügen" hin zur Nutzung von Web 2.0 für Produktivitäts- und Dienstleistungszwecke”*[7], wobei die Aktivitäten einiger Nutzer sozialer Netzwerkdienste unter Umständen über die Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten hinausgehen, so z. B., wenn der soziale Netzwerkdienst als Anwendungsplattform für die Zusammenarbeit eines Verbands, einer Gesellschaft oder eines Unternehmens genutzt wird. Handelt ein Nutzer eines sozialen Netzwerkdienstes für einen Verband, eine Gesellschaft oder ein Unternehmen oder nutzt er den sozialen Netzwerkdienst hauptsächlich als Anwendungsplattform zur Förderung kommerzieller, politischer oder karitativer Zielsetzungen, so findet die Ausnahmeklausel keine Anwendung. Hier übernimmt der Nutzer die volle Verantwortung als „für die Verarbeitung Verantwortlicher“, der einem anderen „für die Verarbeitung Verantwortlichen“, nämlich dem sozialen Netzwerkdienst, und Dritten (anderen Nutzern des sozialen Netzwerkdienstes oder potenziell sogar anderen „für die Verarbeitung Verantwortlichen“ mit Zugriffsmöglichkeiten auf die betreffenden Daten) personenbezogene Daten offenlegt. Unter diesen Umständen benötigt der Nutzer die Einwilligung der betroffenen Personen oder eine sonstige rechtliche Grundlage im Sinne der Datenschutzrichtlinie.

[7] "Internet of the future: Europe must be a key player" („Das Internet der Zukunft: Europa muss ein Leitakteur sein“), Rede von Frau Reding, Mitglied der Europäischen Kommission, zuständig für Informationsgesellschaft und Medien, am 2. Februar 2009 in Brüssel auf der Tagung zur Zukunft der Internetinitiative des Europäischen Rates von Lissabon.

Typischerweise ist der Zugriff auf die von einem Nutzer beigetragenen Daten (Profildaten, publizierte Einträge, Darstellungen und Berichte…) auf die von ihm selbst ausgewählten Kontakte begrenzt. In gewissen Fällen kann ein Nutzer jedoch zu einer hohen Anzahl von Drittkontakten gelangen, von denen er einige unter Umständen gar nicht kennt. Eine hohe Anzahl von Kontakten könnte ein Anhaltspunkt dafür sein, dass die „Ausnahmeklausel für Privathaushalte" keine Anwendung findet und der Nutzer daher als „für die Verarbeitung Verantwortlicher" anzusehen ist.

3.1.2. Zugriff auf Nutzerprofilinformationen

Zum Schutz der Privatsphäre sollten sie sozialen Netzwerkdienste funktionstüchtige datenschutzfreundliche und unentgeltliche Standardeinstellungen sicherstellen, die die Zugriffsmöglichkeiten auf die vom Nutzer selbst ausgewählten Kontakte beschränken.

Reichen die Zugriffsmöglichkeiten auf Profilinformationen über die vom Nutzer selbst ausgewählten Kontakte hinaus, so z. B., wenn allen Mitgliedern des sozialen Netzwerks Zugriff auf ein Profil gewährt wird[8], oder wenn die betreffenden Daten von externen Suchmaschinen indexiert werden können, so geht der Zugriff über die Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten hinaus. Ebenso kommen alle Aufgaben und Pflichten des für die Verarbeitung Verantwortlichen zur Geltung, wenn ein Nutzer in voller Kenntnis der Sachlage die Entscheidung trifft, die Zugriffsmöglichkeit über den Kreis der von ihm selbst ausgewählten „Freunde" hinaus auszudehnen. Effektiv tritt dieselbe Rechtswirkung ein, wenn eine andere Person anderweitige Anwendungsplattformen und -technologien/Programmierschnittstellen benutzt, um personenbezogene Daten im Web zu veröffentlichen[9]. In mehreren Mitgliedstaaten bedeutet der Mangel an Zugriffsbeschränkungen (und somit die öffentliche Eigenschaft), dass die Datenschutzrichtlinie in dem Sinne Anwendung findet, dass der Internetnutzer die Aufgaben und Pflichten des für die Verarbeitung Verantwortlichen erhält[10].

Zu bedenken ist, dass auch dann, wenn die „Ausnahmeklausel für Privathaushalte" nicht greift, der Nutzer sozialer Netzwerkdienste unter weitere Ausnahmeregelungen fallen kann, so beispielsweise unter die Ausnahme der Verarbeitung personenbezogener Daten, die allein zu journalistischen, künstlerischen oder literarischen Zwecken erfolgt. In diesen Fällen ist die Freiheit der Meinungsäußerung gegen das Recht auf Privatsphäre abzuwägen.

3.1.3 Verarbeitung personenbezogener Daten Dritter durch den Nutzer

Die Anwendbarkeit der „Ausnahmeklausel für Privathaushalte" ist auch durch die Notwendigkeit eingeschränkt, die Rechte Dritter zu gewährleisten, so insbesondere im Hinblick auf sensible Daten. Ferner ist darauf hinzuweisen, dass auch dann, wenn die „Ausnahmeklausel für Privathaushalte" anwendbar ist, ein Nutzer nach den allgemeinen Bestimmungen des einschlägigen nationalen Zivil- oder Strafrechts zur Verantwortung gezogen werden kann (so z. B. bei Verleumdung/übler Nachrede: Schadensersatzpflicht wegen Verletzung der Persönlichkeitsrechte, strafrechtliche Verantwortlichkeit).

---

8 Bzw. wenn dargelegt werden kann, dass bei der Akzeptierung von Kontakten keine wirkliche Auswahl getroffen wird, d. h. die Nutzer „Kontakte" unabhängig davon akzeptieren, dass sie mit diesen wirklich in Verbindung stehen.

9 So z. B. bei Publikationsplattformen, die selbst keine SNS sind, oder bei selbst beherbergten Softwareanwendungen.

10 In seinem Urteil Satamedia hat der EuGH in Randnr. 44 im Umkehrschluss für Recht erkannt: *„Demzufolge ist diese zweite Ausnahme dahin auszulegen, dass mit ihr nur Tätigkeiten gemeint sind, die zum Privat- oder Familienleben von Privatpersonen gehören (vgl. Urteil Lindqvist, Randnr. 47). Dies ist bei den Tätigkeiten von Markkinapörssi und Satamedia, durch die die erfassten Daten einer unbegrenzten Zahl von Personen zur Kenntnis gebracht werden sollen, offensichtlich nicht der Fall."*

3.2 Sicherheits- und datenschutzfreundliche Standardeinstellungen

Die Datensicherheit bei der Informationsverarbeitung ist ein entscheidender Faktor für das Vertrauen in soziale Netzwerkdienste. Die für die Verarbeitung personenbezogener Daten Verantwortlichen müssen geeignete technische und organisatorische Maßnahmen treffen, und zwar „sowohl zum Zeitpunkt der Planung des Verarbeitungssystems als auch zum Zeitpunkt der eigentlichen Datenverarbeitung“, um insbesondere deren Sicherheit zu gewährleisten und somit jede unrechtmäßige Verarbeitung zu verhindern, wobei das Schutzniveau den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen sein muss[11].

Ein wichtiger Faktor der Vorgaben und Vorkehrungen zum Schutz der Privatsphäre sind die Zugriffsmöglichkeiten auf die in einem Nutzerprofil enthaltenen personenbezogenen Daten. Wenn es keinerlei Beschränkungen für solche Zugriffsmöglichkeiten gibt, können Dritte entweder als Mitglied des sozialen Netzwerks oder mithilfe von Suchmaschinen allerlei Arten von ganz persönlichen Details über die Nutzer miteinander verknüpfen und zueinander in Beziehung setzen. Bei der Anmeldung bei einem Netzwerkdienst nimmt jedoch nur eine Minderheit von Nutzern Veränderungen an den Standard- und Datenschutzeinstellungen vor. Daher sollten die sozialen Netzwerkdienste datenschutzfreundliche Standardeinstellungen anbieten, die eine Nutzerkontrolle ermöglichen, bei der der Nutzer in jeden Zugriff auf seine Profildaten, der über seine selbst ausgewählten Kontakte hinausreicht, ausdrücklich und ohne Einschränkung einwilligen muss, um somit das Risiko der rechtswidrigen Verarbeitung seiner Daten durch Dritte zu verringern. Die Nutzerprofilinformationen mit beschränkten Zugriffmöglichkeiten sollten nicht durch interne Suchmaschinen aufgespürt werden können, so auch nicht mittels Suchfunktionen nach Parametern wie Alters- oder Ortsangaben. Es darf keine impliziten Entscheidungen über die Ausdehnung der Zugriffsmöglichkeiten geben[12], beispielsweise im Wege einer "Opt-out-Möglichkeit" durch den für die Verarbeitung Verantwortlichen des sozialen Netzwerkdienstes.

3.3 Informationspflichten des sozialen Netzwerkdienstes (SNS)

Die Anbieter sozialer Netzwerkdienste sollten ihre Nutzer nach Maßgabe des Artikels 10 der Datenschutzrichtlinie über ihre Identität aufklären und die gesamte Bandbreite der unterschiedlichen Vorhaben und Zielsetzungen darstellen, die sie mit ihrer Verarbeitung von personenbezogenen Daten verbinden. Dazu gehört zumindest

- die Nutzung der Daten zu Zwecken der Direktwerbung;
- die etwaige gemeinsame Nutzung der Daten mit Dritten, die von ihrer Kategorie her näher zu bezeichnen sind;
- eine Übersicht über die Nutzerprofile: ihre Erstellung und die wichtigsten Datenquellen;
- der Umgang mit sensiblen Daten.

Die Datenschutzgruppe empfiehlt, dass

---

[11] Artikel 17 und Erwägungsgrund 46 der Datenschutzrichtlinie.

[12] Bericht und Empfehlungen zum Datenschutz in sozialen Netzwerkdiensten („Rom-Memorandum“) weisen auf die Risiken hin, wie z. B. auf den „irreführenden Begriff der "Gemeinschaft"“, S. 2, auf die Tatsache, „es könnten mehr personenbezogene Informationen weitergegeben werden als man denkt“, S. 3. Eine Computersicherheitsfirma spricht gegenüber einem bedeutenden SNS eine Warnung in Bezug auf Standardzugriffsmöglichkeiten auf Mitglieder im selben geografischen Gebiet aus: http://www.sophos.com/pressoffice/news/articles/2007/10/facebook-network.html

- die Anbieter sozialer Netzwerkdienste ihre Nutzer beim Hochladen von personenbezogenen Informationen ins soziale Netzwerkprofil angemessen auf die Sicherheitsrisiken für sich und andere in Bezug auf den Schutz der Privatsphäre hinweisen;

- die Nutzer sozialer Netzwerkdienste daran erinnert werden, dass das Hochladen von personenbezogenen Informationen über andere Personen deren Rechte auf Privatsphäre und auf informationelle Selbstbestimmung verletzen kann;

- die Nutzer sozialer Netzwerkdienste von diesen darauf aufmerksam gemacht werden, Bilder oder Informationen über andere Personen nur mit Einwilligung der betroffenen Person hochzuladen[13].

3.4 Sensible Daten

Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie Daten über Gesundheit oder Sexualleben gelten als sensible Daten. Sensible personenbezogene Daten dürfen nur mit der ausdrücklichen Einwilligung des Betroffenen im Internet veröffentlicht werden, es sei denn die betroffene Person hat die Daten offenkundig selbst öffentlich gemacht.[14]

In einigen EU-Mitgliedstaaten gelten die Bilder von betroffenen Personen als spezielle Kategorie personenbezogener Daten, da sie zur Unterscheidung der rassischen/ethnischen Herkunft bzw. zur Herleitung religiöser Überzeugungen oder gesundheitlicher Daten verwendet werden können. Die Datenschutzgruppe betrachtet Bilder im Internet im Allgemeinen nicht als sensible Daten[15], es sei denn die Bilder werden eindeutig zur Offenlegung von sensiblen Daten über Personen verwendet.

Als für die Verarbeitung Verantwortliche dürfen die sozialen Netzwerkdienste keinerlei sensible Daten über Mitglieder und Nichtmitglieder des sozialen Netzwerks ohne deren ausdrückliche Einwilligung verarbeiten[16]. Nimmt ein sozialer Netzwerkdienst in sein Formular zum Nutzerprofil etwaige Fragen zu sensiblen Daten auf, so hat er eindeutig darauf hinzuweisen, dass die Beantwortung dieser Fragen ohne jede Einschränkung auf freiwilliger Basis erfolgt.

3.5 Verarbeitung von Daten von Nichtmitgliedern

Viele soziale Netzwerkdienste gestatten ihren Nutzern Beiträge mit Daten über andere Personen, wie z. B. das Hinzufügen des Namens der abgebildeten Person(en) zum jeweiligen Bild, die Bewertung von Personen, die Erfassung der „Personen, die ich auf Veranstaltungen getroffen habe/gerne treffen möchte“. Diese Kennzeichnung kann auch Nichtmitglieder des Netzwerks kenntlich machen. Jedoch darf die Verarbeitung solcher Nichtmitgliederdaten

---

13 Dies ließe sich durch die Einführung von Kennzeichnungs- und Steuerungssystemen auf den Websites der sozialen Netzwerke vereinfachen, z. B. indem man in einem persönlichen Profil Bereiche ausweist, in denen auf gekennzeichnete Bilder oder Videos hingewiesen wird, da sie mit dem Namen eines Nutzers versehen sind und daher auf seine Einwilligung zur Veröffentlichung warten, oder in denen Verfallsdaten für gekennzeichnete Bilder oder Videos gesetzt werden, die keine Einwilligung der betroffenen Person erhalten haben.

14 Die Mitgliedstaaten können Ausnahmeregelungen erlassen; siehe Artikel 8 Absatz 2 Buchstabe a) 2. Halbsatz und Artikel 8 Absatz 4 der Datenschutzrichtlinie.

15 Die Veröffentlichung von Bildern im Internet erregt jedoch immer mehr Besorgnis im Hinblick auf den Schutz der Privatsphäre, da die Technologien der Gesichtserkennung immer besser werden.

16 Die Einwilligung muss frei, informiert und spezifisch erfolgen.

durch den sozialen Netzwerkdienst nur erfolgen, wenn eines der in Artikel 7 der Datenschutzrichtlinie festgelegten Kriterien erfüllt ist.

Ferner bedarf es für die Generierung von vorgefertigten persönlichen Profilen von Nichtmitgliedern mithilfe der Aggregation der Daten, die von den Nutzern des sozialen Netzwerkdienstes unabhängig voneinander beigetragen wurden, einschließlich der Erstellung von Daten über persönliche Beziehungen oder sachliche Zusammenhänge, die aus hochgeladenen Adressbüchern hergeleitet werden, einer Rechtsgrundlage.[17]

Selbst wenn der soziale Netzwerkdienst Mittel und Wege hätte, um Kontakt mit dem Nichtnutzer aufzunehmen und ihn über das Vorhandensein personenbezogener Daten über ihn zu informieren, würde eine etwaige Einladung an ihn per E-Mail, den sozialen Netzwerkdienst zwecks Zugriffsmöglichkeit auf diese personenbezogenen Daten zu besuchen, gegen das Verbot für das Versenden unerbetener elektronischer Nachrichten zu Zwecken der Direktwerbung nach Artikel 13 Absatz .4 der Datenschutzrichtlinie für elektronische Kommunikation verstoßen.

3.6 Zugriffsmöglichkeiten durch Dritte

3.6.1 Über den sozialen Netzwerkdienst (SNS) vermittelte Zugriffsmöglichkeiten

Neben ihrer eigentlichen Dienstleistung bieten die meisten sozialen Netzwerkdienste ihren Nutzern auch noch Zusatzanwendungen an, die von dritten Software-Entwicklern über Anwendungsprogrammierschnittstellen bereitgestellt werden; diese Drittanbieter verarbeiten ebenfalls personenbezogene Daten.

Die sozialen Netzwerkdienste sollten über Mittel und Wege verfügen, mit denen sichergestellt werden kann, dass die Anwendungen von Drittanbietern im Einklang mit der Datenschutzrichtlinie und der Datenschutzrichtlinie für elektronische Kommunikation stehen. Dies bedeutet insbesondere, dass die Drittanbieter den Nutzern eindeutige und spezifische Informationen über die Verarbeitung ihrer personenbezogenen Daten an die Hand geben, und dass sie nur Zugriff auf die unbedingt notwendigen personenbezogenen Daten haben. Daher sollten die sozialen Netzwerkdienste Drittanbietern abgestufte Zugriffsmöglichkeiten anbieten, so dass diese für ein stärker eingeschränktes Zugriffsverfahren optieren können. Außerdem sollten die sozialen Netzwerkdienste sicherstellen, dass den Nutzern einfache Mechanismen zur Verfügung stehen, mit denen sie ihre Bedenken und Beschwerden über die Anwendungen von Drittanbietern geltend machen können.

3.6.2 Über den Nutzer vermittelte Zugriffsmöglichkeiten Dritter

Die sozialen Netzwerkdienste gestatten ihren Nutzern manchmal den Zugriff und die Aktualisierung ihrer Daten mithilfe anderer Anwendungen. So können Nutzer mitunter

- von ihrem Mobiltelefon aus Nachrichten an das Netzwerk lesen und versenden;
- auf einem Desktop-PC die Kontaktdaten ihrer Freunde im sozialen Netzwerk mit ihrem Adressbuch synchronisieren;
- mittels einer anderen Website ihren Status oder Standort im sozialen Netzwerk automatisch aktualisieren.

[17] Nach Erwägungsgrund 38 der Datenschutzrichtlinie gilt Folgendes: „*Datenverarbeitung nach Treu und Glauben setzt voraus, dass die betroffenen Personen in der Lage sind, das Vorhandensein einer Verarbeitung zu erfahren und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert zu werden, wenn Daten bei ihnen erhoben werden*“. Für einige SNS ist die Veröffentlichung von persönlichen Profilen von Nichtmitgliedern angeblich zu einem wichtigen Standbein der Vermarktung ihrer „Dienstleistungen“ geworden.

Die sozialen Netzwerkdienste veröffentlichen Angaben dazu, wie die Software in Form einer "Anwendungsprogrammierschnittstelle" ("API") beschaffen sein soll. Aufgrund dieser Informationen können Drittanbieter die Software für die Ausführung der betreffenden Aufgaben entwickeln und die Nutzer zwischen mehreren Drittanbietern frei auswählen[18]. Wird eine API angeboten, die den Zugriff auf Kontaktdaten ermöglicht, so sollte der soziale Netzwerkdienst

- für ein Granularitätsniveau sorgen, bei dem der Nutzer die Mindestzugriffsebene für den Dritten bestimmen kann, die gerade noch zur Durchführung einer bestimmten Aufgabe ausreicht.

Wird im Namen des Nutzers über die API eines Dritten auf personenbezogene Daten zugegriffen, so sollte der Drittanbieter

- die betreffenden Daten nicht länger verarbeiten und speichern als dies zur Ausführung der betreffenden Aufgabe nötig ist;

- außer der persönlichen Nutzung durch den Nutzer, der den Beitrag geleistet hat, keinerlei Bearbeitungen an den vom Nutzer eingebrachten Kontaktdaten vornehmen.

3.7 Rechtsgrundlagen für die Direktwerbung

Die Direktwerbung ist wesentlicher Bestandteil des Geschäftsmodells sozialer Netzwerkdienste, wobei diese verschiedene Werbemodelle verfolgen können. Jedoch sollte die Verwendung der personenbezogenen Daten ihrer Nutzer zu Werbezwecken im Einklang mit den einschlägigen Bestimmungen der Datenschutzrichtlinie und der Datenschutzrichtlinie für elektronische Kommunikation stehen[19].

Kontextbezogene Werbung ist auf die Inhalte zugeschnitten, die sich der Nutzer ansieht bzw. auf die er zugreift.[20]

Segmentbezogene Werbung versorgt gewisse Zielgruppen von Nutzern mit Werbeprojektionen[21]; wobei ein Nutzer der betreffenden Gruppe anhand der Informationen zugeordnet wird, die er dem sozialen Netzwerkdienst auf direktem Wege mitgeteilt hat.[22]

Verhaltensbezogene Werbung erfolgt, indem die Werbeprojektionen anhand der Beobachtung und Analyse der Aktivitäten ausgewählt werden, die der Nutzer über einen gewissen Zeitraum an den Tag legt. Je nach den einschlägigen Rechtsgrundlagen und den Merkmalen der eingesetzten Techniken unterliegen diese Techniken mitunter unterschiedlichen rechtlichen Anforderungen. Die Datenschutzgruppe empfiehlt, für verhaltensbezogene Werbemodelle keine sensiblen Daten zu verwenden, sofern nicht alle rechtlichen Anforderungen erfüllt sind.

Welches Modell oder welche Kombination von Modellen auch immer genutzt wird, können Werbeprojektionen entweder direkt durch den sozialen Netzwerkdienst (der Anbieter des sozialen Netzwerkdienstes handelt hierbei als Vermittler) oder durch einen dritten Werbeanbieter eingeblendet werden. Im ersten Fall müssen Dritten gegenüber keinerlei

---

[18] Während es sich bei "API" um einen allgemeinen technischen Begriff handelt, ist unter API hier der Zugriff im Namen des betreffenden Nutzers gemeint, d. h. der Nutzer muss der Software seine Log-in-Berechtigung bekannt geben, damit diese in seinem Namen aktiv werden kann.

[19] Die Datenschutzgruppe beabsichtigt, die verschiedenen Aspekte der Onlinewerbung demnächst in einem eigenen Dokument zu behandeln.

[20] Wenn beispielsweise die aufgerufene Seite den Begriff „Paris“ erwähnt, könnte die betreffende Werbung ein bestimmtes Restaurant in dieser Stadt anpreisen.

[21] Jede Gruppe wird anhand einer Reihe von Kriterien definiert.

[22] Z. B. anlässlich der Anmeldung und Registrierung beim Netzwerkdienst.

personenbezogene Daten des Nutzers offengelegt werden. Im zweiten Fall verarbeitet der Drittwerbeanbieter mitunter jedoch personenbezogene Daten über den Nutzer, so z. B., wenn er die IP-Adresse des Nutzers und ein auf dem Computer des Nutzers befindliches Cookie verarbeitet.

3.8 Vorratsspeicherung von Daten

Soziale Netzwerkdienste fallen nicht in den Geltungsbereich der Definition für elektronische Kommunikationsdienste nach Artikel 2 Buchstabe c) der Richtlinie 2002/21/EG (Rahmenrichtlinie). Die Anbieter sozialer Netzwerkdienste können zusätzliche Dienstleistungen anbieten, die in den Anwendungsbereich eines elektronischen Kommunikationsdienstes fallen, wie z. B. einen öffentlich zugänglichen E-Mail-Dienst. Solche Dienste unterliegen dann der Datenschutzrichtlinie für elektronische Kommunikation und der Datenvorratsspeicherungsrichtlinie.

Einige soziale Netzwerke gestatten ihren Nutzern die Versendung von Einladungen an Dritte. Das Verbot für das Versenden unerbetener elektronischer Nachrichten zu Zwecken der Direktwerbung gilt nicht für persönliche Mitteilungen. Um sich im Rahmen der Ausnahmeregelung für persönliche Mitteilungen zu bewegen, muss ein sozialer Netzwerkdienst die folgenden Kriterien erfüllen:

- weder dem Absender noch dem Empfänger wird ein Anreiz geboten;
- der Anbieter hat hinsichtlich der Empfänger der persönlichen Mitteilung keinerlei Auswahlmöglichkeit;[23]
- die Identität des absendenden Nutzers ist eindeutig anzugeben;
- der absendende Nutzer muss den Inhalt der Mitteilung, die in seinem Namen versandt wird, vollständig kennen.

Einige soziale Netzwerkdienste praktizieren auch eine Vorratsspeicherung von Daten zur Identifizierung der aus dem Netzwerk ausgeschlossenen Nutzer, um sicherzustellen, dass diese sich nicht erneut anmelden und registrieren können. In diesem Fall sind diese ehemaligen Nutzer darüber zu unterrichten, dass eine derartige Verarbeitung von Daten stattfindet. Ferner darf die Vorratsspeicherung nur die Identifizierungsdaten und nicht auch die Gründe für den Ausschluss dieser Personen betreffen. Diese Vorratsspeicherung sollte nicht länger als ein Jahr andauern.

Die von einem Nutzer bei der Anmeldung zum sozialen Netzwerk mitgeteilten personenbezogenen Daten sollten gelöscht werden, sobald entweder der Nutzer oder der Anbieter des sozialen Netzwerkdienstes sich entscheidet, das betreffende Nutzerprofil zu löschen.[24] Genauso sollte mit Informationen, die von einem Nutzer bei der Aktualisierung seines Nutzerprofils gelöscht wurden, keine Vorratsspeicherung erfolgen. Die sozialen Netzwerkdienste sollten ihre Nutzer vor dem Ergreifen solcher Maßnahmen mit den ihnen zur Verfügung stehenden Mitteln unterrichten und sie über den Zeitraum dieser Vorratspeicherung informieren. Aus Sicherheits- und Rechtsgründen könnte es in spezifischen Fällen gerechtfertigt sein, aktualisierte oder gelöschte Daten und Nutzerprofile für einen näher bestimmten Zeitraum zu speichern, um Vorgänge in böswilliger Absicht, die

[23] Beispielsweise ist auch die Praxis einiger sozialer Netzwerkdienste, die Einladungen des Nutzers unterschiedslos an sein gesamtes Adressbuch zu versenden, unzulässig.

[24] Gemäß Artikel 6 Absatz 1 Buchstabe e) der Datenschutzrichtlinie müssen personenbezogene Daten *„nicht länger, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist, in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Person ermöglicht“*.

aus Identitätsdiebstahl und anderen strafbaren oder kriminellen Handlungen resultieren, verhindern zu helfen.

Benutzt ein Nutzer den sozialen Netzwerkdienst für einen bestimmten Zeitraum nicht mehr, so sollte sein Nutzerprofil in den inaktiven Zustand versetzt werden, d. h. für andere Nutzer oder die Außenwelt nicht mehr sichtbar sein; nach Ablauf eines weiteren Zeitraums sollten die Daten in dem aufgegebenen Nutzerprofil gelöscht werden. Die sozialen Netzwerkdienste sollten den Nutzer vor dem Ergreifen dieser Maßnahmen mit den ihnen zur Verfügung stehenden Mitteln unterrichten.

3.9 Rechte der Nutzer

Die sozialen Netzwerkdienste sollten die Rechte der von der Verarbeitung betroffenen Personen im Einklang mit den Bestimmungen der Artikel 12 und 14 der Datenschutzrichtlinie wahren.

Die Zugriffs- und Berichtigungsrechte der Nutzer sind nicht auf die jeweiligen Nutzer des sozialen Netzwerkdienstes begrenzt, sondern erstrecken sich auf alle natürlichen Personen, deren personenbezogene Daten verarbeitet werden.[25] Mitglieder und Nichtmitglieder müssen über Mittel und Wege verfügen, um ihre Rechte auf Zugriff, Berichtigung und Löschung geltend zu machen. Die Homepage des sozialen Netzwerkdienstes sollte klar und deutlich auf die „Beschwerdestelle“ verweisen, die vom Anbieter des sozialen Netzwerkdienstes eingerichtet wurde, um Fragen und Probleme im Zusammenhang mit dem Datenschutz und dem Schutz der Privatsphäre zu klären und den Beschwerden von Mitgliedern wie auch von Nichtmitgliedern nachzugehen.

Nach Artikel 6 Absatz 1 Buchstabe c) der Datenschutzrichtlinie ist darauf zu achten, dass personenbezogene Daten „*den Zwecken entsprechen, für die sie erhoben und/oder verarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen*“. In diesem Zusammenhang lässt sich feststellen, dass es für die sozialen Netzwerkdienste zwar erforderlich sein mag, einige Identifizierungsdaten über ihre Mitglieder zu registrieren, sich daraus aber noch nicht die Notwendigkeit ergibt, den wirklichen Namen ihrer Mitglieder im Internet zu veröffentlichen. Daher sollten die sozialen Netzwerkdienste sorgfältig abwägen, ob sie es rechtfertigen können, ihre Nutzer zu zwingen, im Rahmen ihrer echten Identität anstatt unter einem pseudonymen Profil zu handeln. Es gibt starke Argumente zugunsten einer diesbezüglichen Wahlmöglichkeit der Nutzer, und zumindest in einem Mitgliedstaat ist diese bereits gesetzliches Erfordernis. Besonderes Gewicht kommt diesen Argumenten bei sozialen Netzwerken mit großer Mitgliedschaft zu.

Nach Artikel 17 der Datenschutzrichtlinie hat der für die Verarbeitung Verantwortliche die geeigneten technischen und organisatorischen Sicherheitsmaßnahmen durchzuführen, die für den Schutz personenbezogener Daten erforderlich sind. Zu diesen Sicherheitsmaßnahmen zählen insbesondere Zugriffskontroll- und Authentifizierungsmechanismen, die auch bei der Verwendung von pseudonymen Profilen funktionieren.

[25] Dies ist beispielsweise schon der Fall, wenn die E-Mail-Adresse einer Person vom sozialen Netzwerkdienst benutzt wird, um ihm eine Einladung zu schicken.

4. Kinder und Minderjährige

Ein Großteil der sozialen Netzwerkdienste wird von Kindern/Minderjährigen genutzt. Die Stellungnahme der Datenschutzgruppe WP147[26] befasste sich mit der Anwendung der Datenschutzgrundsätze im Bereich der Schuldaten und Bildungseinrichtungen. In der Stellungnahme wurde die Notwendigkeit betont, das Wohl des Kindes vorrangig zu berücksichtigen, wie dies auch im UN-Übereinkommen über die Rechte des Kindes verankert ist. Die Datenschutzgruppe möchte die Bedeutung dieses zentralen Rechtsgrundsatzes auch im Zusammenhang mit den sozialen Netzwerkdiensten unterstreichen.

Weltweit wurden von den Datenschutzbehörden einige interessante Initiativen[27] unternommen, die sich in der Hauptsache mit der Aufklärung über soziale Netzwerkdienste und mit der Sensibilisierung für die möglichen Risiken ihrer Nutzung befassten. Die Datenschutzgruppe fordert zu weitergehenden Forschungsmaßnahmen zu der Frage auf, wie die Schwierigkeiten im Zusammenhang mit einer geeigneten Altersüberprüfung und Nachweisführung über die informierte Einwilligung in Angriff genommen werden können, um diese Herausforderungen besser zu meistern.

Aufgrund der bisherigen Überlegungen vertritt die Datenschutzgruppe die Auffassung, dass eine Mehrfach-Strategie geeignet ist, den Schutz personenbezogener Daten von Kindern im Zusammenhang mit sozialen Netzwerkdiensten in den Griff zu bekommen. Diese Strategie könnte auf folgenden Faktoren beruhen:

- Aufklärungs- und Sensibilisierungsinitiativen; sie sind von grundlegender Bedeutung, um die aktive Einbeziehung der Kinder sicherzustellen (über die Schulen, die Aufnahme der Vermittlung von Datenschutz-Grundkenntnissen in die Lehrpläne für Schulen und Bildungseinrichtungen, die Anschaffung von eigens zu diesem Zweck ausgearbeiteten Lehr- und Unterrichtsmaterialien, die Zusammenarbeit der zuständigen nationalen Datenschutzeinrichtungen);

- einwandfreie und rechtmäßige Verarbeitung personenbezogener Daten im Hinblick auf Minderjährige, wie z. B. keinerlei Abfragen von sensiblen Daten in den Anmeldeformularen, keine speziell auf Minderjährige ausgerichtete Direktwerbung, Erfordernis der vorherigen Einwilligung der Eltern vor jeder Registrierung, geeignete Grade für die abgestufte Trennung zwischen den Datensätzen der Kinder- und der Erwachsenencommunity;

- Einführung von Technologien zur Stärkung des Schutzes der Privatsphäre (PETs) - z. B. datenschutzfreundliche Standardeinstellungen, Einblendung von Warnsignalen bei sicherheitsrelevanten Schritten, Software zur Altersüberprüfung);

- Selbstkontrolle und –regulierung durch die Anbieter von sozialen Netzwerkdiensten, Förderung der Annahme von praktischen Verhaltenskodexen mit wirksamen Zwangsmaßnahmen und disziplinierenden Wirkungen;

- gegebenenfalls Ad-hoc-Gesetzgebungsmaßnahmen zur Verhinderung unfairer und/oder irreführender Praktiken im Zusammenhang mit sozialen Netzwerkdiensten.

---

[26] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp147_de.pdf

[27] Z. B. die portugiesische Initiative „Dadus“: http://dadus.cnpd.pt/; die dänische Plakette für sicherheitsüberprüftes Chatten: http://www.fdim.dk/

5. Zusammenfassung der Rechte und Pflichten

Anwendbarkeit der EG-Richtlinien

1. Die Datenschutzrichtlinie findet im Allgemeinen auf die Verarbeitung personenbezogener Daten durch soziale Netzwerkdienste (SNS) auch dann Anwendung, wenn diese ihren Hauptsitz außerhalb des EWR haben.

2. Die Anbieter sozialer Netzwerkdienste gelten als für die Verarbeitung Verantwortliche im Sinne der Datenschutzrichtlinie.

3. Die Anbieter von Anwendungssoftware sind unter Umständen als für die Verarbeitung Verantwortliche im Sinne der Datenschutzrichtlinie anzusehen.

4. Die Nutzer gelten in Bezug auf die Verarbeitung ihrer personenbezogenen Daten durch die sozialen Netzwerkdienste als betroffene Personen.

5. Die Verarbeitung personenbezogener Daten durch die Nutzer fällt in den meisten Fällen unter die Ausnahmeklausel für Privathaushalte. Es gibt jedoch auch Fälle, in denen die Tätigkeiten eines Nutzers nicht unter diese Ausnahmeregelung fallen.

6. Soziale Netzwerkdienste fallen nicht in den Geltungsbereich der Definition für elektronische Kommunikationsdienste; somit findet die Datenvorratsspeicherungsrichtlinie auf soziale Netzwerkdienste keine Anwendung.

Pflichten der sozialen Netzwerkdienste (SNS)

7. Die sozialen Netzwerkdienste sollten ihre Nutzer über ihre Identität aufklären und umfassende und eindeutige Informationen über ihre Zielsetzungen sowie über die verschiedenen Möglichkeiten vorlegen, wie sie die personenbezogenen Daten verarbeiten wollen.

8. Die sozialen Netzwerkdienste sollten datenschutzfreundliche Standardeinstellungen anbieten.

9. Die sozialen Netzwerkdienste sollten den Nutzern ausreichende Informationen und geeignete Warnhinweise zu den Risiken für den Schutz ihrer Privatsphäre an die Hand geben, die mit dem Hochladen von personenbezogenen Daten ins soziale Netzwerkprofil verbunden sind.

11. Die Nutzer sollten vom sozialen Netzwerkdienst darauf hingewiesen werden, dass Bilder oder Informationen über dritte Personen nur mit der Einwilligung der betroffenen Person ins soziale Netzwerkprofil eingestellt werden sollten.

12. Die Homepage des sozialen Netzwerkdienstes sollte zumindest einen Link zu einer Beschwerdestelle aufweisen, die sich mit den Datenschutzfragen der Mitglieder wie auch der Nichtmitglieder befasst.

13. Sämtliche Werbemaßnahmen müssen im Einklang mit den einschlägigen Bestimmungen der Datenschutzrichtlinie und der Datenschutzrichtlinie für elektronische Kommunikation stehen.

14. Die sozialen Netzwerkdienste müssen sich festlegen, wie lange die Vorratsspeicherung von Daten inaktiver Nutzer im Höchstfall zulässig ist. Aufgegebene Nutzerprofile sind zu löschen.

15. Im Hinblick auf Minderjährige sollten die sozialen Netzwerkdienste geeignete Maßnahmen zur Begrenzung der Risiken ergreifen.

<u>Rechte der Nutzer</u>

16. Sowohl die Mitglieder als auch die Nichtmitglieder von sozialen Netzwerkdiensten genießen gegebenenfalls die Rechte der betroffenen Person im Sinne der Artikel 10 bis 14 der Datenschutzrichtlinie.

17. Sowohl den Mitgliedern als auch den Nichtmitgliedern sollte im Rahmen des sozialen Netzwerkdienstes ein leicht handhabbares Beschwerdeverfahren zur Verfügung stehen.

18. Den Nutzern sollte es im Allgemeinen gestattet sein, ein Pseudonym anzunehmen.

Brüssel, den 12. Juni 2009
Für die Datenschutzgruppe
Der Vorsitzende
Alex TÜRK