www.jusletter-it.eu

Eva Souhrada-Kirchmayer

EU-Datenschutzrechtliche Aspekte der Sozialen Netzwerke

Die Nutzung sozialer Netzwerke wirft eine Reihe von datenschutzrechtlichen Fragen auf. Neben Fragen des anwendbaren Rechts stellt sich auch jene nach der Sachlichkeit der Ausnahmen von der Richtlinie 95/46/EG und insbesondere auch der geplanten Datenschutz-Grundverordnung der EU. Letztendlich bedürfte es auch eines weltweiten Datenschutzinstruments, um die Durchsetzbarkeit des Rechts zu gewährleiten.

Category: Articles
Region: Austria

Citation: Eva Souhrada-Kirchmayer, EU-Datenschutzrechtliche Aspekte der Sozialen Netzwerke, in: Jusletter IT next: 11. September 2014 – Lachmayer

ISSN 1664-848X, http://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 EDITIONS WEBLAW

Inhaltsübersicht

1 Nutzung sozialer Netzwerke in Österreich

[Rz 1] Ein soziales Netzwerk bzw. Social Network im Internet ist eine lose Verbindung von Menschen in einer Netzgemeinschaft. Handelt es sich um Netzwerke, bei denen die Benutzer gemeinsam eigene Inhalte erstellen, bezeichnet man diese auch als soziale Medien.[1] Das weltweit größte soziale Netzwerk mit über einer Milliarde aktiver Nutzer ist Facebook.[2] Bei der Entwicklung und Nutzung von Sozialen Netzwerken handelt es sich um ein relativ neues Phänomen, wobei die Zahl der Nutzer dieser Websites ständig exponentiell zunimmt.

[Rz 2] Personenbezogene Daten über Einzelne werden öffentlich (und global) in einer nie vorher da gewesenen Weise und Menge verfügbar, insbesondere riesige Mengen digitaler Bilder und Videos.[3] Im Hinblick auf den Schutz der Privatsphäre könnte eine der grundlegendsten Herausforderungen in der Tatsache gesehen werden, dass die meisten der personenbezogenen Informa-

1 Wikipedia, http://de.wikipedia.org/wiki/Soziales_Netzwerk_%28Internet%29(die Zitate der Internetlinks beziehen sich auf den Stichtag 12. April 2013).

2 Facebooks offizielle Statistik, https://newsroom.fb.com/content/default.aspx?NewsAreaId=22.

3 Die Ausführungen in diesem Absatz stammen aus der Stellungnahme der Berliner «International Working Group on Data Protection in Telecommunications» (Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation) dem so genannten «*Rom-Memorandum*»,http://www.datenschutz.fu-berlin.de/dahlem/ressourcen/675_36_13-ROM-Memorandum.pdf.

tionen, die in sozialen Netzwerkdiensten publiziert werden, auf Initiative der Nutzer selbst und mit ihrer Einwilligung veröffentlicht werden. Während die «traditionelle» Datenschutzgesetzgebung sich mit der Definition von Regeln zum Schutz der Bürger gegen unfaire oder unverhältnismäßige Verarbeitung personenbezogener Daten durch die öffentliche Verwaltung (einschließlich Strafverfolgungsbehörden und Geheimdienste), und von Unternehmen beschäftigt, gibt es nur sehr wenige Regelungen zur Veröffentlichung personenbezogener Daten auf Initiative der Betroffenen selbst, weil dies vor der Entwicklung sozialer Netzwerkdienste weder in der «Offline-Welt» noch im Internet ein großes Problem darstellte. Außerdem ist die Verarbeitung personenbezogener Daten aus öffentlichen Quellen traditionell in der Datenschutzgesetzgebung privilegiert.

[Rz 3] 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 Nutzung sozialer Netzwerke wirft daher grundsätzliche Datenschutzfragen auf. Die auf den Webportalen sozialer Netzwerke bekannt gegebenen personenbezogenen Daten lassen sich von unbefugten Dritten für verschiedenste Vorhaben und Zielsetzungen ausnutzen, so auch für kommerzielle Zwecke, und bergen in sich mit unter größere Gefahren und Risiken, wie z. B. Identitätsdiebstahl, finanzielle Einbußen, Nachteile für Geschäfts- oder Erwerbsmöglichkeiten und Beeinträchtigung der körperlichen Unversehrtheit.[4]

[Rz 4] Obwohl 34% der Österreicher und Österreicherinnen soziale Netzwerke nutzen,[5] spielen diese im «täglichen Leben» der österreichischen Datenschutzkommission keine zentrale Rolle. Dies liegt vor allem daran, dass die Regelung des § 3 DSG 2000 (in Umsetzung des Art. 4 der Datenschutzrichtlinie 95/46/EG[6]) eine Regelung enthält, wonach dann, wenn ein ausländischer Auftraggeber des privaten Bereichs einen Sitz in einem anderen Mitgliedstaat der Europäischen Union hat und personenbezogene Daten in Österreich zu einem Zweck verwendet, der keiner in Österreich gelegenen Niederlassung dieses Auftraggebers zuzurechnen ist, das Recht des Sitzstaates des Auftraggebers auf eine Datenverarbeitung im Inland anzuwenden ist.[7]

[Rz 5] Nachdem der größte Anbieter Sozialer Netzwerke «Facebook» jedenfalls eine Niederlassung in Dublin (Irland) hat,[8] ist für Beschwerden gegen Facebook, soweit die Datenverarbeitung

---

4 Stellungnahme 5/2009 der Art. 29 Datenschutzgruppe zur Nutzung sozialer Online-Netze (WP 163), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_de.pdf, 4.

5 http://derstandard.at/1345165045996/Nutzung-von-Internet-und-sozialen-Netzwerken-stagniert.

6 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 281/31 vom 23.11.1995 (im Folgenden: «DSRL»).

7 §3 Abs. 2 DSG 2000. § 3 DSG 2000 lautet: **Räumlicher Anwendungsbereich § 3.**(1) Die Bestimmungen dieses Bundesgesetzes sind auf die Verwendung von personenbezogenen Daten im Inland anzuwenden. Darüber hinaus ist dieses Bundesgesetz auf die Verwendung von Daten im Ausland anzuwenden, soweit diese Verwendung in anderen Mitgliedstaaten der Europäischen Union für Zwecke einer in Österreich gelegenen Haupt- oder Zweigniederlassung (§ 4 Z 15) eines Auftraggebers (§ 4 Z 4) geschieht. (2) Abweichend von Abs. 1 ist das Recht des Sitzstaates des Auftraggebers auf eine Datenverarbeitung im Inland anzuwenden, wenn ein Auftraggeber des privaten Bereichs (§ 5 Abs. 3) mit Sitz in einem anderen Mitgliedstaat der Europäischen Union personenbezogene Daten in Österreich zu einem Zweck verwendet, der keiner in Österreich gelegenen Niederlassung dieses Auftraggebers zuzurechnen ist. (3) Weiters ist dieses Bundesgesetz nicht anzuwenden, soweit personenbezogene Daten durch das Inland nur durchgeführt werden. (4) Von den Abs. 1 bis 3 abweichende gesetzliche Regelungen sind nur in Angelegenheiten zulässig, die nicht dem Recht der Europäischen Gemeinschaften unterliegen.

8 Ein weiterer Sitz Facebooks befindet sich in Deutschland (Facebook Germany); in einem Rechtsstreit zwischen Facebook und dem Landeszentrum für Datenschutz Schleswig-Holstein bekam Facebook mit zwei Beschlüssen vom 14. Februar 2013 des Verwaltungsgerichts Schleswig (Az. 8 B 60/12, 8 B 61/12) jedoch Recht «Das Datenschutzzentrum habe seine Anordnung zu Unrecht auf das deutsche Datenschutzrecht gestützt. Dieses sei jedoch nicht anwendbar. Nach der DSRL und dem Bundesdatenschutzgesetz finde das deutsche Recht keine Anwendung, so-

für Zwecke dieser Niederlassung erfolgt, die irische Datenschutzbehörde zuständig. Diese hat ihre Zuständigkeit bereits in mehreren Fällen anerkannt. Berühmt geworden ist vor allem die von österreichischen Studenten gegründete Initiative «Europe versus Facebook»[9]: eine Gruppe österreichischer Studenten, als deren Sprecher Max Schrems auftrat, brachten bei der irischen Datenschutzbehörde 22 Beschwerdepunkte gegen Facebook ein. Die irische Behörde leitete ein Verfahren gegen Facebook ein und erteilte Empfehlungen an Facebook, denen teilweise Folge geleistet wurde.[10]

[Rz 6] Dennoch kann man nicht von einem gänzlichen Ausschluss der Anwendbarkeit österreichischen Rechts ausgehen, zumal auch die Nutzer selbst als Auftraggeber tätig werden können.[11]

[Rz 7] Im folgenden Beitrag sollen vor allem die europarechtlichen Datenschutzaspekte dargestellt werden.

2 Datenschutzrechtliche Überlegungen auf europäischer Ebene

[Rz 8] Zu den europarechtlichen Datenschutzaspekten bezüglich sozialer Netzwerkdienste wurden schon von verschiedenen Institutionen Überlegungen getätigt, und zwar aus verschiedenen Blickpunkten aus und in verschiedener Tiefe.

[Rz 9] Bereits im Oktober 2007 veröffentlichte die Europäische Agentur für Netz- und Informationssicherheit (ENISA) das Positionspapier «*Security Issues and Recommendations for Online Social Networks» (Sicherheitsfragen und Empfehlungen für Soziale Online-Netzwerke)*, das sich an Gesetzgeber, Anbieter und Nutzer sozialer Netzwerke richtet.[12]

[Rz 10] Im März 2008 verabschiedete die Berliner «International Working Group on Data Protection in Telecommunications» (Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation) das so genannte «*Rom-Memorandum*», 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.[13]

---

fern die Erhebung und Verarbeitung von personenbezogenen Daten durch eine Niederlassung in einem anderen Mitgliedstaat der Europäischen Union stattfinde. Dies sei hier der Fall: Die Facebook Ltd. Ireland erfülle mit dem dort vorhandenen Personal und den dortigen Einrichtungen alle Voraussetzungen einer Niederlassung in diesem Sinne mit der Folge, dass ausschließlich irisches Datenschutzrecht Anwendung finde. Die Facebook Germany GmbH hingegen sei ausschließlich im Bereich der Anzeigenaquise und des Marketing tätig. Daher sei sowohl die Anordnung der Entsperrung als auch die Zwangsgeldandrohung rechtswidrig.», siehe http://www.schleswig-holstein.de/OVG/DE/Service/Presse/Pressemitteilungen/15022013VG_facebook_anonym.html, Verwaltungsgericht gibt Eilanträgen von Facebook statt.

9 http://www.europe-v-facebook.org/DE/de.html.

10 Europe-v-Facebook veröffentlichte unter http://www.europe-v-facebook.org/report.pdfeinen Gegenbericht zum Bericht der irischen Datenschutzbehörde, da nach Meinung der Beschwerdeführer noch einige Empfehlungen nicht befolgt wurden und Beschwerdepunkte offen geblieben waren.

11 Siehe dazu auch die Ausführungen von Leissler,Soziale Netzwerke und Datenschutzrecht, in: Jahrbuch Datenschutzrecht 11, *Jahnel*(Hg), Wien 2011, 111f. Insofern ist eine gewisse Diskrepanz zwischen der Interpretation der Art. 29 Datenschutzgruppe (siehe die Ausführungen unter Punkt 2.2. zum anwendbaren Recht und Punkt 2.3. zur datenschutzrechtlichen Rollenverteilung), wonach ein Nutzer im persönlich-familiären Bereich gar nicht als «für die Verarbeitung Verantwortlicher» zu sehen ist, und der österreichischen Rechtslage, wonach auch Nutzer prinzipiell unter die Regelungen des DSG 2000 fallen und — sofern sie Daten über Dritte verarbeiten — als Auftraggeber gelten., deren Tätigkeit allerdings unter Umständen unter die Bestimmung des § 45 DSG 2000 fällt und daher z. B. von der Meldepflicht an die Datenschutzkommission befreit ist.

12 http://www.enisa.europa.eu/publications/archive/soc-net.

13 ROM-Memorandum, aaO.

[Rz 11] Auch die «*Entschließung zum Datenschutz in sozialen Netzwerkdiensten*» (angenommen von der 30. Internationalen Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre in Straßburg am 17. Oktober 2008), stellt auf die mit diesen Diensten einhergehenden Herausforderungen ab.[14]

[Rz 12] Schließlich verabschiedete die so genannte «Art. 29 Datenschutzgruppe» im Juni 2009 eine «*Stellungnahme zur Nutzung sozialer Online-Netzwerke*» *(WP 163).*[15]

2.1 Definition und Geschäftsmodell der «sozialen Netzwerkdienste»

[Rz 13] Die Art. 29 Datenschutzgruppe definiert soziale Netzwerke als «Kommunikationsplattformen im Online-Bereich, die es dem Einzelnen ermöglichen, sich Netzwerken von gleich gesinnten Nutzern anzuschließen bzw. solche zu schaffen».[16] Im rechtlichen Sinne handle es sich bei den sozialen Netzwerken um Dienstleistungen der Informationsgesellschaft im Sinne Richtlinie über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften.

[Rz 14] «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) 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.

[Rz 15] 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.»[17]

[Rz 16] Wie die Berlin- Gruppe feststellt, sind soziale Netzwerke «nicht — wie vielleicht der Ausdruck ‹sozial› nahe legen könnte — öffentliche Versorgungsbetriebe.»[18] Die Dienste seien daher «kostenlos, aber nicht umsonst.» Tatsache ist, dass die Nutzer sozialer Netzwerke zwar nicht finanziell zur Kasse gebeten werden, sondern mit ihren personenbezogenen Daten zahlen.

[Rz 17] Es ist daher wichtig, dass soziale Netzwerkdienste datenschutzkonform 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 europäi-

14 http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/IntDSK/2008Soziale Netzwerke.html?nn=409246.

15 Die folgenden Ausführungen in Kapitel 2 basieren im Wesentlichen auf den Ausführungen der Art. 29 Datenschutzgruppe.

16 WP 163, aaO, 5.

17 WP 163, aaO, 5.

18 ROM-Memorandum, aaO, 3.

schen und dem einzelstaatlichen Datenschutzrecht sowie der einschlägigen Gesetzgebung zum Schutz der Privatsphäre verarbeitet werden.[19]

2.2 Anwendbares Recht

[Rz 18] Die Art. 29 Datenschutzgruppe weist darauf hin, dass in den meisten Fällen auch für die Anbieter von sozialen Netzwerken die Bestimmungen der Datenschutzrichtlinie 95/46/EG (im Folgenden «DSRL») gelten, und zwar sogar auch dann, wenn ihr Hauptsitz außerhalb des EWR liege. Im Übrigen wird auf die Ausführungen in ihrer Stellungnahme zu Datenschutzfragen im Zusammenhang mit Suchmaschinen verwiesen.[20]

[Rz 19] In dieser Stellungnahme zu den Suchmaschinen wird unter anderem Folgendes ausgeführt: «Bei der Verarbeitung personenbezogener Daten durch einen Anbieter, der in einem oder in mehreren Mitgliedstaaten niedergelassen ist und all seine Dienstleistungen dort erbringt, fällt die Verarbeitung personenbezogener Daten eindeutig in den Anwendungsbereich der DSRL. In diesem Fall ist es wichtig zu beachten, dass die Datenschutzbestimmungen nicht auf die betroffenen Personen im Hoheitsgebiet oder mit einer Staatsangehörigkeit eines der Mitgliedstaaten beschränkt sind.

[Rz 20] Ist der Suchmaschinenbetreiber ein nicht im EWR ansässiger für die Verarbeitung Verantwortlicher, so ist das gemeinschaftliche Datenschutzrecht in zwei Fällen dennoch anwendbar, und zwar erstens, wenn der Suchmaschinenbetreiber eine Niederlassung in einem Mitgliedstaat im Sinne von Artikel 4 Absatz 1 Buchstabe a besitzt, und zweitens, wenn die Suchmaschine auf Mittel im Hoheitsgebiet eines Mitgliedstaats im Sinne von Artikel 4 Absatz 1 Buchstabe c zurückgreift. Im zweiten Fall muss der Suchmaschinenbetreiber gemäß Artikel 4 Absatz 2 einen im Hoheitsgebiet des genannten Mitgliedstaats ansässigen Vertreter benennen.»[21]

[Rz 21] Eine «Niederlassung»[22] setzt die effektive und tatsächliche Ausübung einer Tätigkeit unter dauerhaften Bedingungen voraus. Die Rechtsform der Niederlassung — eine Geschäftsstelle, eine Tochtergesellschaft mit Rechtspersönlichkeit oder eine Vertretung durch Dritte — ist dabei nicht entscheidend.

[Rz 22] Eine weitere Forderung ist jedoch, dass der Verarbeitungsvorgang «im Rahmen der Tätigkeiten» einer *Niederlassung* ausgeführt wird. Das bedeutet, dass die Niederlassung ebenfalls eine bedeutende Rolle bei dem betreffenden Verarbeitungsvorgang spielen sollte.

[Rz 23] «Dies ist eindeutig der Fall, wenn:

- eine Niederlassung für die Beziehungen zu den Benutzern des Anbieters in einem bestimmten gerichtlichen Zuständigkeitsbereich verantwortlich ist;
- ein Anbieter ein Büro in einem Mitgliedstaat (EWR) einrichtet, das am Verkauf zielgruppenspezifischer Werbeanzeigen an die Einwohner dieses Staates beteiligt ist;
- die Niederlassung eines Anbieters in Bezug auf Benutzerdaten richterlichen Anordnungen

19 WP 163, aaO, 5.

20 «Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen», angenommen am 4. April 2008 (WP148), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_de.pdf.

21 WP 148, aaO, 10.

22 Ausführungen zur «Niederlassung» finden sich bereits im Arbeitspapier über die Frage der internationalen Anwendbarkeit des EU-Datenschutzrechts bei der Verarbeitung personenbezogener Daten im Internet durch Websites außerhalb der EU (WP 56), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp56_de.pdf, 8f.

und/oder Ersuchen der zuständigen Behörden eines Mitgliedstaats zur Strafverfolgung nachkommt.

[Rz 24] Suchmaschinen, die im Hoheitsgebiet eines Mitgliedstaats (EWR) für die Verarbeitung von personenbezogenen Daten auf Mittel zurückgreifen, fallen ebenfalls in den Anwendungsbereich der Datenschutzgesetze dieses Mitgliedstaats.»[23]

[Rz 25] Die Datenschutzgesetze eines Mitgliedstaats sind auch noch anwendbar, wenn der für die Verarbeitung Verantwortliche «*[. . .] zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurückgreift, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind, es sei denn, dass diese Mittel nur zum Zweck der Durchfuhr durch das Gebiet der Europäischen Gemeinschaft verwendet werden.*»[24]

[Rz 26] «Was die Bereitstellung von Suchmaschinendiensten außerhalb der EU anbetrifft, so können im Hoheitsgebiet eines Mitgliedstaats befindliche Datenzentren für die Speicherung und Fernverarbeitung personenbezogener Daten genutzt werden. Weitere Beispiele für Mittel sind der Einsatz von Personalcomputern, Endgeräten und Servern. Die Verwendung von Cookies und ähnlichen Softwareinstrumenten durch einen Anbieter von Online-Diensten kann ebenfalls als Rückgriff auf Mittel im Hoheitsgebiet eines Mitgliedstaats angesehen werden, was somit die Anwendung der Datenschutzgesetze des betreffenden Mitgliedstaats erfordert.»[25]

[Rz 27] Dieser Punkt war bereits im Arbeitspapier WP 56 erörtert worden: «*Wie bereits gesagt, kann der PC eines Nutzers als ein Mittel im Sinne von Artikel 4 Absatz 1 Buchstabe c der Richtlinie 95/46/EG angesehen werden. Er befindet sich im Gebiet eines Mitgliedstaats. Der für die Verarbeitung Verantwortliche hat beschlossen, dieses Mittel zum Zwecke der Verarbeitung personenbezogener Daten zu nutzen. Wie bereits in den vorstehenden Absätzen erläutert, laufen jetzt einige technische Operationen ab, die nicht unter der Kontrolle der betroffenen Person stehen. Der für die Verarbeitung Verantwortliche verfügt damit über die Mittel des Nutzers und diese Mittel werden nicht nur zum Zwecke der Durchfuhr durch das Gebiet der Gemeinschaft verwendet.*» [26]

[Rz 28] Aus den Ausführungen der Art. 29 Datenschutzgruppe wird ersichtlich, dass diese ein relativ weites Verständnis vom zweiten Tatbestand des Art. 4 Abs. 1 lit. c DSRL hat, das wohl bei manchen Drittstaaten auf Widerstand stößt.

2.3 Datenschutzrechtliche Rollenverteilung[27]

2.3.1 Anbieter sozialer Netzwerkdienste

[Rz 29] Die Anbieter sozialer Netzwerkdienste sind die «für die Verarbeitung von Benutzerdaten Verantwortlichen» im Sinne der DSRL.[28] 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

[23] WP 148, aaO, 11.

[24] WP 148, aaO, 12.

[25] WP 148, aaO, 12.

[26] WP 56, aaO, 12.

[27] Das folgende Kapitel gibt die Ausführungen der Art. 29-Datenschutzgruppe wieder, siehe WP 163, aaO, 6ff.

[28] Der im österreichischen DSG 2000 definierte «Auftraggeber» entspricht dem in der DSRL verwendeten Begriff des «für die Verarbeitung Verantwortlichen».

Nutzung der Benutzerdaten zu Werbe- und Vermarktungszwecken — so auch durch dritte Werbeanbieter.

2.3.2 Anbieter von Anwendungs-/Softwaredienstleistungen

[Rz 30] 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.

2.3.3 Nutzer

[Rz 31] Nach Meinung der Art. 29 Datenschutzgruppe sind in den meisten Fällen die Nutzer als «betroffene Personen» anzusehen. Die Pflichten des «für die Verarbeitung Verantwortlichen» finden nach der DSRL 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.[29]

[Rz 32] Bei den sozialen Netzwerkdiensten gebe es nämlich 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*», 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 benötige der Nutzer die Einwilligung der betroffenen Personen oder eine sonstige rechtliche Grundlage im Sinne der DSRL.[30]

[Rz 33] 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» an-

[29] WP 163, aaO, 6.

[30] WP 163, aaO, 6.

zusehen ist.[31]

[Rz 34] Wie von der Art. 29 Datenschutzgruppe ausgeführt wird, sollten die sozialen Netzwerkdienste zum Schutz der Privatsphäre 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, 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. Der Mangel an Zugriffsbeschränkungen (und somit die öffentliche Eigenschaft) bewirkt, dass die DSRL in dem Sinne Anwendung findet, dass der Internetnutzer die Aufgaben und Pflichten des für die Verarbeitung Verantwortlichen erhält. Aber 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.

[Rz 35] Im Dokument WP 163 der wird auch darauf hingewiesen, dass die Anwendbarkeit der «Ausnahmeklausel für Privathaushalte» auch durch die Notwendigkeit eingeschränkt wird, *die Rechte Dritter zu gewährleisten*, so insbesondere im Hinblick auf sensible Daten.[32] 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 Strafrecht zur Verantwortung gezogen werden kann (so z. B. bei Verleumdung/übler Nachrede: Schadensersatzpflicht wegen Verletzung der Persönlichkeitsrechte, strafrechtliche Verantwortlichkeit).[33]

2.4 Rechtsgrundlagen

2.4.1 Zustimmung der Betroffenen

[Rz 36] Als Rechtsgrundlage kommt bei sozialen Netzwerken grundsätzlich wohl am ehesten die Zustimmung der betroffenen Person in Frage. Nach Art. 4 lit. h DSRL ist unter der «Einwilligung der betroffenen Person» *jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene*

31 WP 163, aaO, 7.

32 Hier wird allerdings nicht gesagt, aufgrund welcher datenschutzrechtlicher Rechtsgrundlage eine Achtung der Rechte Dritter geboten ist, da ja nach dem Verständnis der Gruppe die Anwendbarkeit der Ausnahme für Privathaushalte gar keine Auftraggebereigenschaft begriündet.

33 WP 163, aaO, 7.

Daten, die sich betreffen, verarbeitet werden.» Hier können sich in einigen Fällen berechtigter Weise Zweifel ergeben, inwieweit eine Zustimmung «in Kenntnis der Sachlage» gegeben ist. Wenn Zustimmungserklärungen derart aufgebaut sind, dass die geplanten Datenanwendungen nur in schwer verständlichen und teils intransparenten Begleittexten dargelegt werden (wie es bei Social Networks oft der Fall ist), so erscheint es fraglich, inwieweit derartige Zustimmungen schon strukturell einen validen Rechtfertigungstatbestand darstellen können.[34]

2.4.2 Erheblichkeit der Daten

[Rz 37] Nach Art. 6 Abs. 1 lit. c) DSRL müssen 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. Es stellt sich daher die Frage, ob soziale Netzwerke ihre Nutzer zwingen dürfen, im Rahmen ihrer echten Identität anstatt unter einem pseudonymen Profil zu handeln. Besonderes Gewicht kommt dieser Frage bei sozialen Netzwerken mit großer Mitgliedschaft zu. Wie die Art. 29 Datenschutzgruppe ausführt, hat nach Art. 17 der DSRL 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.[35] Insoweit stellt sich die Frage, ob die Verpflichtung zur Verwendung des Klarnamens dem Verhältnismäßigkeitsprinzip entspricht. Daraus kann wohl gefolgert werden, dass soziale Netzwerke die Verwendung von Pseudonymen zulassen sollte.

2.5 Verpflichtungen der Netzwerkbetreiber[36]

2.5.1 Datenschutzfreundliche Standardeinstellungen[37]

[Rz 38] Ein wichtiger Beitrag 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 («Privacy by default») anbieten, die eine Nutzerkontrolle ermöglichen. Dabei müsste jeder Nutzer in jeden Zugriff auf seine Profildaten, der über seine selbst ausgewählten Kontakte hinausreicht, ausdrücklich und ohne Einschränkung einwil-

34 Sinngemäß *Leissler*, Soziale Netzwerke und Datenschutzrecht, aaO, 14f.

35 WP 163, aaO, 13.

36 Siehe dazu WP 163, aaO, 8ff.

37 WP 163, aaO, 8 und ROM-Memorandum, aaO, 7f.

ligen, 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, beispielsweise im Wege einer «Opt-out-Möglichkeit» durch den für die Verarbeitung Verantwortlichen des sozialen Netzwerkdienstes.

2.5.2 Informationspflichten des sozialen Netzwerkdienstes

[Rz 39] Die Anbieter sozialer Netzwerkdienste müssen ihre Nutzer nach Maßgabe des Art. 10 DSRL über ihre Identität aufklären und die gesamte Bandbreite der unterschiedlichen Vorhaben und Zielsetzungen darstellen, die sie mit ihrer Verarbeitung von personenbezogenen Daten verbinden. Es muss sichergestellt werden, dass Diensteanbieter in ehrlicher und klarer Weise darlegen, welche Daten für den Basisdienst erforderlich sind, so dass die Nutzer eine informierte Wahl treffen können, ob sie den Dienst in Anspruch nehmen wollen oder nicht.[38] Die Informationspflicht umfasst auch 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 sowie den Umgang mit sensiblen Daten.[39]

2.6 Rechte der Nutzer

2.6.1 Betroffenenrechte

[Rz 40] Die sozialen Netzwerkdienste sind verpflichtet, die Rechte der von der Verarbeitung betroffenen Personen im Einklang mit den Bestimmungen der Art. 12 und 14 DSRL zu wahren. Es handelt sich hiebei um die Betroffenenrechte auf Auskunftserteilung, Richtigstellung und Löschung sowie um das Widerspruchsrecht. Die Betroffenenrechte sind nicht auf die jeweiligen Nutzer des sozialen Netzwerkdienstes begrenzt, sondern erstrecken sich auf alle natürlichen Personen, deren personenbezogene Daten verarbeitet werden. Mitglieder und Nichtmitglieder müssen über Mittel und Wege verfügen, um ihre Rechte auf Auskunft, Berichtigung und Löschung geltend zu machen. Die Art. 29 Datenschutzgruppe fordert, dass die Homepage des sozialen Netzwerkdienstes klar und deutlich auf die «Beschwerdestelle» verweisen sollte, 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.[40]

[Rz 41] Wie sich in der Praxis gezeigt hat, gestaltet sich die Ausübung der Betroffenenrechte in der Praxis schwierig: So berichtete Max Schrems, nach anfänglichen Schwierigkeiten von Facebook etwa 1200 Seiten von Daten übermittelt bekommen zu haben, wobei diese Daten einerseits nicht vollständig gewesen seien; andererseits seien auch bereits gelöscht geglaubte Daten in diesem

38 ROM-Memorandum, aaO, 5.

39 WP 163, aaO, 8.

40 WP 163, aaO, 13.

Konvolut enthalten gewesen.[41]

2.6.2 Kinder und Minderjährige[42]

[Rz 42] Die Art. 29 Datenschutzgruppe vertritt die Auffassung, dass (nur) 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 Aufklärungs- und Sensibilisierungsinitiativen beruhen; 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.

3 Ausgewählte Rechtsprobleme — insbesondere im Hinblick auf den Entwurf einer Datenschutz-Grundverordnung

3.1 Vorschläge neuer EU-Rechtsinstrumente im Datenschutz

[Rz 43] Die Europäische Kommission hat am 25. Jänner 2012 den Entwurf einer Datenschutz-Grundverordnung[43] vorgestellt, die die DSRL ablösen soll, sowie den Entwurf einer Richtlinie für den Bereich der ehemaligen «Dritten Säule» (Zusammenarbeit von Polizei und Justiz in Strafsa-

41 http://www.spiegel.de/netzwelt/web/facebook-kritiker-mein-gesicht-ist-nicht-deren-geschaeftsgeheimnis-a-789124.html.

42 Siehe WP 163, aaO, 14.

43 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, KOM(2012) 11 endgültig, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF.

chen)[44], die den Rahmenbeschluss «Datenschutz»[45] ablösen soll. Die Entwürfe für die beiden neuen Rechtsinstrumente sind Gegenstand intensiver Verhandlungen in der Ratsarbeitsgruppe «Datenschutz» («RAG DAPIX») und dem Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres (so genannter «LIBE-Ausschuss») im Europäischen Parlament.[46] Für die Verwendung sozialer Netzwerke wird vor allem die Datenschutz-Grundverordnung eine besondere Rolle spielen.

3.2 Einwilligung

[Rz 44] Die Art. 29-Datenschutzgruppe hat eine ausführliche Stellungnahme zur Frage der «Einwilligung» abgegeben.[47] Nach Ansicht der Art 29 Datenschutzgruppe ist für die Erteilung der Zustimmung immer eine Aussage («statement») oder eine Handlung («action») notwendig, und reines Schweigen («mere silence») oder eine Unterlassung («inaction») können keine Zustimmung darstellen. Beispielhaft wird auf ein Soziales Netzwerk verwiesen und explizit ausgeführt:

> «***Beispiel: Privatsphäre-Voreinstellungen***
>
> *Die Voreinstellungen in privaten Netzwerken, auf die Nutzer nicht unbedingt Zugriff nehmen müssen, um das Netzwerk zu nutzen, ermöglichen die gesamte ‹Friend of a Friend› Kategorie, bei der die personenbezogenen Daten jedes Nutzers allen ‹Friends of a Friend› sichtbar gemacht werden. Nutzer, die nicht möchten, dass ihre personenbezogenen Daten von ‹Friends of a Friend› gesehen werden, müssen eine Schaltfläche anklicken. Wenn sie passiv bleiben oder die Schaltfläche nicht anklicken, geht der für die Datenverarbeitung Verantwortliche davon aus, dass sie eingewilligt haben, dass ihre Daten sichtbar sind. Es ist jedoch sehr fraglich, ob das Nicht- Anklicken einer Schaltfläche bedeutet, dass die Nutzer im Allgemeinen einwilligen, ihre Informationen allen ‹Friends of a Friend› sichtbar zu machen. Aufgrund der Unsicherheit, ob das Ausbleiben einer Handlung wirklich als Einwilligung gemeint ist, kann das Nicht-Anklicken nicht als Einwilligung ohne Zweifel gelten.*»[48]

[Rz 45] Der Entwurf der Datenschutz-Grundverordnung soll die Betroffenenrechte in der Online-Umgebung stärken[49] und sieht hiefür verschiedene Maßnahmen vor. Eine davon ist eine Neuregelung der Einwilligung: Als Einwilligung gilt nunmehr eine «explizite Willensbekundung» in Form einer Erklärung oder einer sonstigen eindeutigen Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten

---

44 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, KOM(2012) 10 endgültig, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:DE:PDF.

45 Rahmenbeschluss 2008/977/JI vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl L 350. 60ff..

46 Stand am Stichtag 12. April 2013.

47 Stellungnahme15/2011 zur Definition von Einwilligung (WP 187), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_de.pdf.

48 WP 187, aaO, 22.

49 DieStärkung der Rechte des Einzelnen war bereits im Strategiepapier der Europäischen Kommission im Jahre 2010 enthalten; siehe Mitteilung der Kommission über ein Gesamtkonzept für den Datenschutz in der Europäischen Union an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen vom 4. November 2010, KOM(2010) 609 endgültig, 5ff; . siehe dazu auch *Souhrada-Kirchmayer*, Das Gesamtkonzept der EU für den Datenschutz, Jahrbuch Datenschutzrecht 2011, *Jahnel*(Hg), Wien 2011, 33 ff.

einverstanden sind.[50] Das heißt, eine «implizite» Zustimmung wird es in Zukunft nicht mehr geben.

[Rz 46] Überdies stellt sich nach der geltenden Rechtslage die Frage, ab wann die Einwilligung eines Minderjährigen überhaupt gültig ist. Hier gibt es bislang europaweit keine einheitlichen Regelungen. Selbst im innerstaatlichen Bereich ist es unklar, wo eine derartige Altersgrenze verlaufen könnte: Während manche Kommentare — wohl nicht ganz der Realität Rechnung tragend — auf die Erreichung der Volljährigkeit abstellen,[51] stellen andere auf die Einsichtsfähigkeit ab[52] (was wiederum eine Beurteilung im Einzelfall bedeuten würde). Aus Art. 8 der Datenschutz-Grundverordnung würde sich nun ergeben, dass Minderjährige ab 13 Jahren eine gültige Einwilligung geben können. Diese Frist scheint zwar willkürlich — so würde sich in Österreich etwa das Abstellen auf das Erreichen des Alters der «Mündig Minderjährigen» mit 14 Jahren anbieten — und scheint die Handschrift von «Facebook» zu tragen; auf der anderen Seite würde diese wenigstens erstmals europaweite Klarheit bringen.[53]

3.3 Stärkung der Betroffenenrechte

[Rz 47] Im Entwurf einer Datenschutz-Grundverordnung sind auch die größtenteils bereits bestehenden Betroffenenrechte geregelt, wie das Recht auf Auskunftserteilung, Richtigstellung und Löschung. Genannt ist in diesem Kapitel auch die Informationspflicht des Auftraggebers gegenüber dem Betroffenen. Zu großen (nicht immer nachvollziehbaren) Diskussionen hat das «Recht auf Vergessenwerden und auf Löschung» geführt, das wohl als Kontrapunkt zu dem Satz «Das Internet kennt keine Vergessen» gemeint war. Dahinter verbirgt sich jedoch — im Gegensatz zu früheren Intentionen[54] grundsätzlich (nur) ein detailliert geregeltes Löschungsrecht. Die Regelung scheint aber insofern ambitioniert, als auch jene Personen, die die Daten erhalten haben, möglichst von einer Löschung verständigt werden und ebenso selbst eine Löschung dieser Daten vornehmen sollen.[55]

[Rz 48] Neu ist das Recht auf Datenübertragbarkeit, das in Art. 18 des Entwurfes der Datenschutz-Grundverordnung geregelt ist.[56] Wenn die Zurverfügungstellung von Daten auf Einwilligung oder einem Vertrag beruht, hat die Person das Recht, die zur Verfügung gestellten Daten in einem gängigen Format in ein anderes System zu überführen. Im Übrigen scheint die Bestimmung allerdings relativ unklar, was wohl auch ein Grund dafür war, dass der für die Datenschutz-Grundverordnung zuständige Berichterstatter Jan Philipp Albrecht in seinem Berichtentwurf vorschlägt, das Recht als eine Spezifizierung des Auskunftsrechts in den entsprechenden Arti-

50 Art. 4 Abs. 8 Datenschutz-Grundverordnung.

51 *Dohr/Pollirer/Weiss/Knyrim*, DSG2, Anmerkung zu § 4 Z 14.

52 Z. B. *Zscherpe*, Anforderungen an die datenschutzrechtliche Einsichtsfähigkeit im Internet, MMR 2004, München, 724.

53 Siehe dazu auch die Überlegungen von *Kastelitz/Neugebauer*, Aspekte der datenschutzrechtlichen Zustimmung(sfähigkeit) Minderjähriger, in: Jahrbuch Datenschutzrecht 2011, *Jahnel*(Hg), Wien 2011, 71ff.

54 Siehe Stellungnahme des Europäischen Datenschutzbeauftragten zur Mitteilung der Europäischen Kommission zum «Gesamtkonzept für den Datenschutz in der Europäischen Union», ABl vom 22. Juni 2011, C 181, Rz. 88, in der eine Art «Verfallsdatum» für Daten nach Ablauf einer gewissen Frist angedacht wird.

55 Art. 17 Datenschutz-Grundverordnung, aaO.

56 Dieser lautet: «*Werden personenbezogene Daten elektronisch in einem strukturierten gängigen elektronischen Format verarbeitet, hat die betroffene Person das Recht, von dem für die Verarbeitung Verantwortlichen eine Kopie der verarbeiteten Daten in einem von ihr weiter verwendbaren strukturierten gängigen elektronischen Format zu verlangen.*»

kel, der das Auskunftsrecht regelt, zu inkorporieren.[57]

[Rz 49] Weitere Bestimmungen der Datenschutz-Grundverordnung enthalten Regelungen zur Einschränkung der Erstellung von Persönlichkeitsprofilen[58], der Verpflichtung der für die Verantwortung Verantwortlichen zur Verwendung von datenschutzfreundlichen Technologien und Einstellungen *(«Privacy by design and by default»)*[59] und zur Meldung von Datenschutzverstößen an die Aufsichtsbehörde bzw. allenfalls an die Betroffenen *(«Data breach notification»)*[60].

3.4 Anwendungsbereich der Datenschutz-Grundverordnung

3.4.1 Sachlicher Anwendungsbereich — Ausnahme für Privathaushalte

[Rz 50] Wie im Dokument WP 163 der Art. 29 Datenschutzgruppe dargestellt wurde, fallen Nutzer von sozialen Netzwerken im Regelfall unter die so genannte «Ausnahme für Privathaushalte» (englisch «*household exemption*», Datenverwendung für den persönlich-familiärer Lebensbereich). Die DSRL gilt zwar nicht für Datenanwendungen für persönlich-familiäre Zwecke, schließt aber auch nicht aus, dass dafür Regelungen geschaffen werden. Dementsprechend findet sich im DSG 2000 die Bestimmung des § 45 DSG 2000, die für derartige Datenverwendungen keine Meldepflicht vorsieht, aber doch gewisse Grundregeln aufstellt. Hintergrund der Bestimmung ist, dass Privatpersonen bei Datenanwendungen im persönlich-familiären Lebensbereich keine administrativen Bürden auferlegt werden sollen, aber diese sehr wohl den Datenschutz anderer Personen respektieren müssen.

[Rz 51] Der Entwurf der Datenschutz-Grundverordnung nimmt unter anderem die Verarbeitung personenbezogener Daten, die «*durch natürliche Personen zu ausschließlich persönlichen oder familiären Zwecken ohne jede Gewinnerzielungsabsicht» vorgenommen wird*», vom Anwendungsbereich der Verordnung aus.[61]

[Rz 52] Ein gänzliches «Hinauskippen» derartiger Daten aus der Datenschutz-Grundverordnung würde wohl dazu führen, dass es für derartige Datenverwendungen gar keine Datenschutzregeln mehr gäbe. Es bestünde hier die Gefahr, dass — ohne die Zustimmung der Betroffenen einzuholen — auch personenbezogene Daten über andere publiziert oder an größere Gruppen weitergegeben werden.

[Rz 53] Auf der anderen Seite kennt das auf in Art. 8 der Grundrechte-Charta verankerte Grundrecht auf Datenschutz keine «Ausnahme für Privathaushalte», es scheint zweifelhaft, ob eine gesetzliche Ausnahmeregelung (was die gegenständliche Verordnung dann wohl wäre) überhaupt sachlich gerechtfertigt wäre und dem Verhältnismäßigkeitsprinzip entsprechen würde. Für die Verwendung von Daten für diese Zwecke müssten ME gewisse Grundregeln in der Datenschutz-Grundverordnung normiert werden. Die von der Europäischen Kommission vorgeschlagene Aus-

57 Entwurf eines Berichts über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), 2012/0011(COD), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-501.927%2b04%2bDOC%2bPDF%2bV0%2f%2fDE, Änderungsantrag 142 und 154.

58 Art. 20 des Vorschlags für eine Datenschutz-Grundverordnung, aaO.

59 Art. 23 des Vorschlags für eine Datenschutz-Grundverordnung, aaO.

60 Art. 31 und 32 des Vorschlags für eine Datenschutz-Grundverordnung, aaO.

61 Art. 2 Abs. 2 lit. d des Vorschlags zur Datenschutz-Grundverordnung, aaO.

nahme scheint zu weit zu gehen.

[Rz 54] Andererseits könnte die Einschränkung «ohne Gewinnerzielungsabsicht» wiederum zu eng sein. Eine Streichung der Einschränkung «ohne jede Gewinnerzielungsabsicht» (wie dies der Berichterstatter MEP Jan Philipp Albrecht in seinem Berichtsentwurf vorschlägt[62]) würde wohl durchaus Sinn machen, allerdings unter der Bedingung, dass für die Datenverwendungen im persönlich-familiären Lebensbereich zumindest gewisse minimale Grundregeln des Datenschutzes (Datenschutzgrundsätze und Verwendungsvoraussetzungen) gelten müssen.

3.4.2 Räumlicher Anwendungsbereich und Zuständigkeit der Datenschutz-Aufsichtsbehörden

[Rz 55] Zum nach der DSRL anwendbaren Recht siehe oben, Punkt 2.2.

[Rz 56] Was die Stellung der Datenschutzkontrollstellen betrifft, so ist derzeit — vor allem bei grenzüberschreitendem Bezug — nur eine vage Zusammenarbeitsbestimmung in Art. 28 Abs. 6 DSRL enthalten.[63]

[Rz 57] Die in der Datenschutz-Grundverordnung stellt einerseits auf die Niederlassung eines für die Verarbeitung Verantwortlichen in der EU ab, andererseits wird geregelt, dass die Verordnung Anwendung auf die Verarbeitung personenbezogener Daten von in der Union ansässigen betroffenen Personen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen findet, wenn die Datenverarbeitung dazu dient, diesen Personen in der Union Waren oder Dienstleistungen anzubieten oder der Beobachtung ihres Verhaltens dient. Die Verordnung findet auch Anwendung auf jede Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen an einem Ort, der nach internationalem Recht dem Recht eines Mitgliedstaats unterliegt.[64]

[Rz 58] In Zukunft würde es überdies eine einheitliche Verordnung für den Bereich der EU geben, sodass nicht mehr zu klären wäre, das Recht welchen Mitgliedstaates hier anzuwenden wäre.

[Rz 59] Wohl aber würde sich in Zukunft weiterhin die Frage stellen, welche Datenschutzbehörde zuständig sei. Der Verordnungsentwurf sieht ein «one stop shop» für den Fall vor, dass es mehrere Niederlassungen innerhalb der EU gibt. Diesfalls ist die Aufsichtsbehörde des Mitgliedstaats, in dem sich die Hauptniederlassung des für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters befindet, unbeschadet der Bestimmungen von Kapitel VII dieser Verordnung für die Aufsicht über dessen Verarbeitungstätigkeit in allen Mitgliedstaaten zuständig.[65]

---

62 2012/0011 (COD), aaO, Änderungsvorschlag 79.

63 Art. 28 Abs. 6 DSRL, aaO.

64 Art. 3 der Entwurfes einer Datenschutz-Grundverordnung lautet: 1. Die Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt. 2. Die Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von in der Union ansässigen betroffenen Personen durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen, wenn die Datenverarbeitung a) dazu dient, diesen Personen in der Union Waren oder Dienstleistungen anzubieten, oder b) der Beobachtung ihres Verhaltens dient. 3. Die Verordnung findet Anwendung auf jede Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen an einem Ort, der nach internationalem Recht dem Recht eines Mitgliedstaats unterliegt.

65 Art. 4 (13) des Vorschlages zur Datenschutz-Grundverordnung «Hauptniederlassung» im Falle des für die Verarbeitung Verantwortlichen der Ort seiner Niederlassung in der Union, an dem die Grundsatzentscheidungen hinsichtlich der Zwecke, Bedingungen und Mittel der Verarbeitung personenbezogener Daten getroffen werden; wird über die Zwecke, Bedingungen und Mittel der Verarbeitung personenbezogener Daten nicht in der Union entschieden, ist die Hauptniederlassung der Ort, an dem die Verarbeitungstätigkeiten im Rahmen der Tätigkeiten einer Niederlassung eines für die Verarbeitung Verantwortlichen in der Union hauptsächlich stattfinden. Im Falle des Auftragsverarbei-

[Rz 60] Im Fall Facebook wäre wohl — solange es sich um Datenverarbeitungen «im Rahmen der Niederlassung Facebook Ireland» handelt — wiederum die irische Datenschutzbehörde zuständig.

[Rz 61] Weiters ist im Verordnungsentwurf eine sehr komplexe Regelung zur Zusammenarbeit der Datenschutz-Aufsichtsbehörden enthalten.[66] Nach der künftigen Regelung (Kohärenzmechanismus) wäre Folgendes geboten:

- Die Beschwerde kann bei jeder Datenschutzbehörde eingebracht werden.
- Es besteht eine obligatorische Zusammenarbeit mit anderen Datenschutzbehörden (Gemeinsame Maßnahmen der Aufsichtsbehörden); jede Aufsichtsbehörde, in deren Sitzstaat sich Betroffene befinden, hat das Recht, an den Audits teilzunehmen;
- Es besteht eine obligatorische Befassung des Europäischen Datenschutzausschusses (das ist das Nachfolgegremium der Art. 29 Datenschutzgruppe);
- Eine einheitliche Anwendung und Interpretation der Verordnung ist notwendig — Differenzen würden im Europäischen Datenschutzausschuss ausdiskutiert werden; in bestimmten Fällen besteht sogar eine Interventionsmöglichkeit der Europäischen Kommission;
- Die Datenschutz-Aufsichtsbehörde hat die Möglichkeit der Verhängung von Strafen im Falle von «Non-Compliance».

[Rz 62] Im Verordnungsentwurf ist darüber hinaus sogar die Möglichkeit vorgesehen, dass eine Aufsichtsbehörde stellvertretend für den Betroffenen eine andere Aufsichtsbehörde klagen kann.[67] Diese Bestimmung scheint problematisch, da sie geeignet scheint, die Kooperation und die Vertrauensbasis zwischen den Aufsichtsbehörden grundlegend zu beeinträchtigen.

[Rz 63] Von besonderer Bedeutung wird jedoch in Hinkunft die einheitliche Interpretation der Verordnung und der allgemeinen europäischen Verfahrensgrundsätze sein, da sonst wiederum keine einheitliche Rechtsanwendung und damit kein harmonisiertes Vorgehen stattfinden würde.

3.5 Durchsetzbarkeit

[Rz 64] Naturgemäß kann eine EU-weite Verordnung nicht die Durchsetzbarkeit aller Betroffenenrechte gegenüber «mit der Verarbeitung Verantwortlichen», die sich im Ausland befinden, gewährleisten. Solange diese eine Niederlassung in der EU haben, scheint das Problem teilweise entschärft. Grundsätzlich stellt sich aber nach wie vor die Frage nach einem weltweiten Datenschutzinstrument. Als Ansätze sind etwa die «Madrid-Standards»[68] zu nennen, die 2009 auf der Internationalen Datenschutzkonferenz in Madrid von den unabhängigen Datenschutzbehörden angenommen wurden. Diese stellen allerdings nicht einklagbares «soft law» dar.

[Rz 65] Der Europarat weist regelmäßig darauf hin, dass die bereits seit 1981 bestehende Daten-

ters bezeichnet «Hauptniederlassung» den Ort, an dem der Auftragsverarbeiter seine Hauptverwaltung in der Union hat.

66 Kapitel VII «Zusammenarbeit und Kohärenz» Datenschutz-Grundverordnung, aaO.

67 Art. 74 Abs. 4 Datenschutz-Grundverordnung, aaO.

68 International Standards on the Protection of Personal Data and Privacy, The Madrid Resolution, International Conference of Data Protection and Privacy Commissioners, http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/ common/2009_Madrid/estandares_resolucion_madrid_en.pdf.

schutzkonvention («Konvention 108»)[69], die derzeit modernisiert wird,[70] auch Drittstaaten außerhalb Europas zum Beitritt offen steht. Damit steht ein verbindliches Rechtsinstrument zur Verfügung, das einfache Datenschutzprinzipien enthält. Allerdings spielt hier wohl auch die «psychologische Komponente» eine gewisse Rolle, die Staaten außerhalb Europas davon abhält, einem europäischen Rechtsinstrument beizutreten. Dennoch hat nunmehr als erster außereuropäischer Staat Uruguay den Beitritt zur Konvention 108 beantragt.[71]

4 Zusammenfassung

[Rz 66] Die Nutzung sozialer Netzwerke wirft eine Reihe von datenschutzrechtlichen Fragen auf. Der Vorschlag einer Datenschutz-Grundverordnung soll Probleme, die sich speziell bei der Datenverwendung in der Online-Umgebung ergeben, lösen. Eine Verbesserung ist im Bereich der Zustimmung und der Betroffenenrechte sowie in den Verpflichtungen der mit der Verarbeitung Verantwortlichen zu sehen. Probleme können sich aus dem sachlichen Anwendungsbereich ergeben. Insbesondere bleibt offen, wo die Verwendung für «persönlich-familiäre Zwecke» endet und inwieweit hier die Rechte Dritter gewährleistet werden können. Das Prinzip des one-stop-shops bei der Zuständigkeit von Datenschutzbehörden kann nur dann funktionieren, wenn ein einheitliches Verständnis der Datenschutz-Grundverordnung und der allgemeinen Verfahrensgrundsätze gewährleistet ist. Die Frage der Rechtsdurchsetzung gegen im EU-Ausland befindliche «für die Verarbeitung Verantwortliche» bedarf eines weltweiten Datenschutzinstruments.

5 Literatur

Stellungnahme der Berliner «International Working Group on Data Protection in Telecommunications» (Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation) dem so genannten «*Rom-Memorandum*», http://www.datenschutz.fu-berlin.de/dahlem/ressourcen/675_36_13-ROM-Memorandum.pdf

Stellungnahme 5/2009 der Art. 29 Datenschutzgruppe zur Nutzung sozialer Online-Netze, WP163, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_de.pdf

Der Standard, http://derstandard.at/1345165045996/Nutzung-von-Internet-und-sozialen-Netzwerken-stagniert

Leissler Günter, Soziale Netzwerke und Datenschutzrecht, in: Jahrbuch Datenschutzrecht 11, *Jahnel* (Hrsg.), Wien 2011, 103ff.

«*Security Issues and Recommendations for Online Social Networks*» *(Sicherheitsfragen und Empfehlungen für Soziale Online-Netzwerke)*, http://www.enisa.europa.eu/publications/archive/soc-net

Entschließung zum Datenschutz in sozialen Netzwerkdiensten, http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/IntDSK/2008SozialeNetzwerke.html?nn=409246

69 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108.

70 Bei Redaktionsschluss hatte bereits der beratende Ausschuss nach der Konvention 108 (so genanntes «T-PD») eine Neuregelung angenommen, die aber noch weitere Gremien des Europarates durchlaufen muss.

71 http://www.humanrightseurope.org/2013/04/uruguays-accession-to-convention-108-signals-boost-for-global-data-protection/.

Stellungnahme 1/2008 der Art. 29 Datenschutzgruppe zu Datenschutzfragen im Zusammenhang mit Suchmaschinen, angenommen am 4. April 2008 (WP148), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_de.pdf

Initiative «Europe versus Facebook», http://www.europe-v-facebook.org/DE/de.html

Arbeitspapier der Art. 29 Datenschutzgruppe über die Frage der internationalen Anwendbarkeit des EU-Datenschutzrechts bei der Verarbeitung personenbezogener Daten im Internet durch Websites außerhalb der EU (WP 56), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp56_de.pdf

Der Spiegel, http://www.spiegel.de/netzwelt/web/facebook-kritiker-mein-gesicht-ist-nicht-deren-geschaeftsgeheimnis-a-789124.html

Stellungnahme 15/2011 der Art. 29 Datenschutzgruppe zur Definition von Einwilligung (WP 187), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_de.pdf

Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, KOM(2012) 11 endgültig, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:PDF

Souhrada-Kirchmayer, Eva, Das Gesamtkonzept der EU für den Datenschutz, in: Jahrbuch Datenschutzrecht 2011, *Jahnel* (Hrsg.), Wien 2011, 33ff.

Dohr/Pollirer/Weiss/Knyrim, DSG^2, Kommentar zum Datenschutzgesetz 2000.

Zscherpe, Kerstin A., Anforderungen an die datenschutzrechtliche Einsichtsfähigkeit im Internet, Multimedia und Recht (MMR), München 2004, 723ff.

Kastelitz, Markus/Neugebauer, Carina, Aspekte der datenschutzrechtlichen Zustimmung(sfähigkeit) Minderjähriger, in: Jahrbuch Datenschutzrecht 2011, *Jahnel* (Hrsg.). Wien 2011, 71 ff.

Stellungnahme des Europäischen Datenschutzbeauftragten zur Mitteilung der Europäischen Kommission zum «Gesamtkonzept für den Datenschutz in der Europäischen Union», ABl. vom 22. Juni 2011, C 181/1ff.

Entwurf eines Berichts über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), *Jan Philipp Albrecht*, 2012/0011(COD), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-501.927+04+DOC+PDF+V0//DE, Änderungsantrag 142 und 154

International Standards on the Protection of Personal Data and Privacy, The Madrid Resolution, International Conference of Data Protection and Privacy Commissioners, http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf

http://www.humanrightseurope.org/2013/04/uruguays-accession-to-convention-108-signals-boost-for-global-data-protection/

Eva Souhrada-Kirchmayer, Geschäftsführendes Mitglied und Leiterin der Geschäftsstelle der Datenschutzkommission, Wien, Österreich. Der vorliegende Beitrag stellt eine erweiterte Fassung eines Vortrages dar, den die Autorin anlässlich einer Veranstaltung zum Europäischen Daten-

schutztag 2013 im Bundeskanzleramt gehalten hat. Meine ersten Kontakte mit Friedrich «Friedl» Lachmayer hatte ich bereits zu jener Zeit, als ich noch im Bundesministerium für Wissenschaft und Forschung arbeitete (1983 bis 1991). Als ich 1991 in den BKA-VD eintrat, verstärkte sich die Zusammenarbeit mit dem Jubilar. Schließlich wurden wir zu «Abteilungsleiter-Kollegen», die stets ein freundschaftliches Verhältnis verband. Auch in seinem «Unruhe-Stand» treffe ich immer wieder mit dem Jubilar zusammen — sei es bei Rechtsinformatik-Tagungen oder bei gesellschaftlichen Ereignissen — wobei mir die humorvollen, manchmal philosophischen Bemerkungen Dr. Lachmayers und die Art, wie er manche Dinge direkt, aber nie verletzend auf den Punkt bringt, immer wieder neue Denkanstöße geben.