ULD · Postfach 71 16 · 24171 Kiel

Verwaltungsgericht Schleswig
Brockdorff-Rantzau-Straße 13
24837 Schleswig

Vorab per Telefax: 04621/861277

Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223
Ansprechpartner/in:
Herr Dr. Polenz
Durchwahl: 988-1200

Aktenzeichen:
LD4-61.41/12.004

Kiel, 18. Januar 2013

Verwaltungsrechtssache Unabhängiges Landeszentrum für Datenschutz ./. Facebook Ireland Ltd.; Az.: 8 B 60/12; Ihr Schreiben vom 20. Dezember 2012

Sehr geehrte Damen und Herren,

auf den Antrag der Facebook Ireland Ltd. erwidern wir wie folgt:

1. Anwendung des deutschen Datenschutzrechts

Die Antragstellerin möchte die Anwendung irischen Datenschutzrechts mit Verweis auf Art. 4 Abs. 1 a) Satz 1 der Richtlinie 95/46/EG begründen. Demnach wendet jeder Mitgliedstaat die Vorschriften, die er zur Umsetzung dieser Richtlinie erlässt, auf alle Verarbeitungen personenbezogener Daten an, die im Rahmen der Tätigkeiten einer Niederlassung ausgeführt werden, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet dieses Mitgliedstaats besitzt. Die Prüfung der Voraussetzungen von Art. 4 Abs. 1 a) Satz 1 und 2 der Richtlinie 95/46/EG führt jedoch zur Anwendung des deutschen Datenschutzrechts.

a) Keine Anwendung deutschen Datenschutzrechts durch Rechtswahlklausel

Die Antragstellerin trägt auf Seite 10 ihres Schriftsatzes vom 20. Dezember 2012 vor, dass das Datenschutzrecht als Teil des öffentlichen Rechts nicht zur Disposition der Vertragsparteien steht. Die Antragsgegnerin hat sich mit der in dieser Hinsicht vertretenen Auffassung kritisch auseinandergesetzt. Im Ergebnis wird an der in der Anordnung vom 14. Dezember 2012 vertretenen Ansicht nicht mehr festgehalten. Die Ausführungen der Antragstellerin erscheinen insoweit zutreffend, als darauf hingewiesen wurde, dass die Regelungen zur zivilrechtlichen Rechtswahlvereinbarung im Hinblick auf öffentliches Datenschutzrecht nicht anwendbar sind (Schriftsatz der Antragstellerin vom 20. Dezember 2012, S. 10, 1. Absatz).

b) Verantwortlichkeit für die Datenverarbeitung der Facebook Germany GmbH

Am 11. Februar 2010 richtete Facebook in Deutschland eine eigene Niederlassung ein, die Facebook Germany GmbH (Facebook Germany GmbH, Großer Burstah 50-52, 20457 Hamburg). Nach Darstellung der Antragstellerin agiert die Facebook Germany GmbH nur als Verkaufsstelle. Das Tochterunternehmen erfülle zusätzlich Funktionen bei der Kommunikation mit der Antragstellerin und der Facebook Inc., bei der Werbung und hinsichtlich der Öffentlichkeitsarbeit. An Entscheidungen bezüglich der Datenverarbeitung sei die deutsche Tochter nicht involviert. Dessen ungeachtet berichtet der irische Datenschutzbeauftragte von Datenverarbeitungsverträgen zwischen der Antragstellerin als verantwortliche Stelle und Facebook UK, Schweden, Italy, Germany, France und Netherlands (Report of Audit vom 21. Dezember 2011, S. 25 (**Anlage 1**), abrufbar: http://dataprotection.ie/viewdoc.asp?DocID=1182&m=f. Was sich hinter diesen Verträgen verbirgt, wurde bisher von der Antragstellerin nicht offengelegt.

Bei der in Deutschland bestehenden Niederlassung der Antragstellerin handelt es sich im Verhältnis zur Konzernmutter Facebook Inc. um die inländische Vertreterin nach § 1 Abs. 5 S. 2 BDSG. Voraussetzung für diese Vertretung ist nicht, dass eine besondere Form der Verantwortlichkeit bei der Vertretung besteht. Es genügt, dass diese Erklärungen für die verantwortliche Stelle entgegen nimmt und abgibt. Dies ist bei der Facebook Germany GmbH der Fall. Dass Facebook Inc. sowie dessen deutsche Tochter nicht der Pflicht nach § 1 Abs. 5 S. 3 BDSG nachgekommen ist, Angaben über die Vertretung zu machen, ist für die Annahme des Vertretungsverhältnisses unschädlich.

Nach Auffassung der Antragsgegnerin handelt es sich bei der Facebook Germany GmbH zugleich eine Niederlassung der Antragstellerin im Sinne von § 1 Abs. 5 S. 1 BDSG. Zwar bestreiten sämtliche Facebook-Unternehmen eine Datenverarbeitung durch die deutsche Tochter. Hierauf kommt es aber nicht an. Gemäß Erwägungsgrund 19 der Richtlinie 95/46/EG genügt für die Annahme einer Niederlassung eine „effektive und tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung“. Weiter wird klargestellt, dass es nicht auf die Rechtsform ankommt. Eine selbständige GmbH ist also mit erfasst, was auch eindeutig die weiteren Ausführungen des Erwägungsgrundes belegen: „Wenn der Verantwortliche im Hoheitsgebiet mehrerer Mitgliedstaaten niedergelassen ist, insbesondere mit einer Filiale, muss er vor allem zur Vermeidung von Umgehungen sicherstellen, dass jede dieser Niederlassungen die Verpflichtungen einhält, die im jeweiligen einzelstaatlichen Recht vorgesehen sind, das auf ihre jeweiligen Tätigkeiten anwendbar ist.“ Es ist in der Literatur unbestritten, dass für die Annahme einer Niederlassung eine „nennenswerte Tätigkeit“ genügt, etwa durch eine Ladenfiliale. Sinn und Zweck der Norm ist der Schutz des Betroffenen, weshalb grundsätzlich von einem weiten Niederlassungsbegriff ausgegangen werden muss (Dammann, in: Simitis, Kommentar zum BDSG, 7. Aufl. 2011, § 1 Rn. 203). Zur Eingrenzung des Begriffs der „Niederlassung“ kann auch auf § 42 Abs. 2 GewO zurückgegriffen werden, wonach eine Niederlassung vorhanden ist, wenn der Gewerbetreibende einen zum dauernden Gebrauch eingerichteten, ständig oder in regelmäßiger Wiederkehr von ihm benutzten Raum für den Betrieb seines Gewerbes besitzt (Gola/Schomerus, Kommentar zum BDSG, 11. Aufl. 2012, § 1 Rn 28). Dies trifft auf die Facebook Germany GmbH zu.

Die Annahme der Niederlassung für die Antragstellerin in Form der Facebook Germany GmbH führt dazu, dass im Hinblick auf die Verantwortlichkeit nach § 1 Abs. 5 Satz 1 BDSG

deutsches Datenschutzrecht anzuwenden ist.

Dieses Ergebnis folgt zudem aus der Anwendung von Art. 4 Abs. 1 a) Satz 2 der Richtlinie 95746/EG. Demnach gilt: Wenn der Verantwortliche eine Niederlassung im Hoheitsgebiet mehrerer Mitgliedstaaten besitzt, ergreift er die notwendigen Maßnahmen, damit jede dieser Niederlassungen die im jeweils anwendbaren einzelstaatlichen Recht festgelegten Verpflichtungen einhält. Die Antragstellerin muss als verantwortliche Stelle nach Art. 2 d) der Richtlinie 95/46/EG dafür Sorge tragen, dass die Facebook Germany GmbH als deren Niederlassung deutsches Datenschutzrecht und vor allem die datenschutzrechtlichen Bestimmungen des TMG einhält. Nach Maßgabe von Art. 2 d), 4 Abs. 1 a) Satz 2 der Richtlinie 95/46/EG ist sie zudem selbst verpflichtet, deutsches Datenschutzrecht einzuhalten.

2. Antragsgegnerin ist zuständige Datenschutzaufsichtsbehörde

Maßgebend für die Bestimmung der sachlichen Zuständigkeit für den Erlass der Anordnung ist zunächst Art. 28 Abs. 6 Satz 1 der Richtlinie 95/46/EG. Danach ist jede Kontrollstelle im Hoheitsgebiet ihres Mitgliedstaats für die Ausübung der ihr nach Art. 28 Abs. 3 der Richtlinie 95/46/EG übertragenen Befugnisse zuständig, unabhängig vom einzelstaatlichen Recht, das auf die jeweilige Verarbeitung anwendbar ist. Maßgebend ist aus Sicht der Antragsgegnerin Art. 4 Abs. 1 Satz 2 a) der Richtlinie 95/46/EG. Die Antragstellerin als aus Datenschutzsicht verantwortliche Stelle muss für Niederlassungen in Deutschland die notwendigen Maßnahmen ergreifen, damit diese die im deutschen Datenschutzrecht festgelegten Verpflichtungen eingehalten werden. Für die Facebook Germany GmbH als Niederlassung der Antragstellerin gelten deutsches Datenschutzrecht und vor allem die Bestimmungen des TMG. Die entsprechenden gesetzlichen Regelungen müssen in Erfüllung der Verpflichtung aus Art. 4 Abs. 1 Satz 2 a) der Richtlinie 95/46/EG von der Antragstellerin beachtet und deren Einhaltung bei der Facebook Germany GmbH überprüft werden.

Die sachliche Zuständigkeit der Antragsgegnerin ergibt sich zudem aus § 38 Abs. 1 BDSG i.V.m. § 1 Abs. 5 Satz 1 BDSG. Nach § 38 Abs. 1 Satz 1 BDSG kontrolliert die Aufsichtsbehörde die Ausführung „dieses Gesetzes“ sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln einschließlich des Rechts der Mitgliedstaaten in den Fällen des § 1 Abs. 5 BDSG. Damit sind auch Datenerhebungen, -verarbeitungen und -nutzungen erfasst, die verantwortliche Stellen mit Sitz in einem anderen Mitgliedstaat aus Datenschutzsicht zu verantworten haben. Nur auf diese Weise können die allgemeinen Persönlichkeitsrechte der Bürger gewahrt und das entsprechende gesetzgeberische Anliegen in § 1 Abs. 1 BDSG erfüllt werden.

In Bezug auf die Facebook Ireland Ltd. erläuterte der irische Datenschutzbeauftragte in seinem Bericht aus 2011, dass seine Bestätigung der Zuständigkeit für die Facebook Ireland Ltd. nicht dahingehend verstanden werden darf, er habe die ausschließliche Zuständigkeit über Facebooks Aktivitäten in der Europäischen Union (Report of Audit vom 21. Dezember 2011, S. 21 (Anlage 3). Vielmehr sei der Facebook Ireland Ltd. von September 2010 an eine "verstärkte Verantwortlichkeit" hinsichtlich der Nutzer außerhalb von USA und Kanada zugewiesen worden (Report of Audit vom 21. Dezember 2011, S. 25 (Anlage 3).

3. § 13 Abs. 6 TMG findet für die Antragstellerin Anwendung

a) Anliegen des Richtliniengebers in der Richtlinie 95/46/EG

Entgegen der Darstellung der Antragstellerin beinhaltet § 13 Abs. 6 TMG einen Grundsatz, welcher aus der Richtlinie 95/46/EG ableitbar ist. Die Vorschrift konkretisiert das Ziel der Datenvermeidung, wonach Diensteanbieter im Rahmen der technischen Möglichkeiten den Nutzern anonymes oder pseudonymes Handeln ermöglichen müssen (BT-Drs. 13/7385, S. 23). Das Gebot der Datenvermeidung gilt für den gesamten Nutzungsvorgang. Einer Vollharmonisierung des Datenschutzrechts steht § 13 Abs. 6 TMG nicht entgegen. Vielmehr bestimmt Art. 6 Abs. 1 c) der Richtlinie, dass personenbezogene Daten den Zwecken entsprechen müssen, für die sie erhoben und /oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen. Bereits mit dieser Bestimmung, welche auf die Erforderlichkeit der Datenverarbeitung Bezug nimmt, wird der Grundsatz der Datensparsamkeit konkretisiert. Ferner bestimmt Art. 6 Abs. 1 e) der Richtlinie 95/46/EG, dass 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 Personen ermöglicht. Die Aufbewahrung in besonderen „Formen“ zeigt deutlich, dass der Richtliniengeber Maßnahmen der Anonymisierung und der Pseudonymisierung mit in den Regelungsbereich der Richtlinie aufgenommen hat (Dammann/Simitis, Kommentar zur EG-Datenschutzrichtlinie, 1. Aufl., 1997, Art. 6, Erl. 17; Ehmann/Helfrich, Kommentar zur EG-Datenschutzrichtlinie, Art. 6, Rn. 28 ff.). Schließlich kann das Prinzip einer datenvermeidenden Angebots- und Technikgestaltung auf Erwägungsgrund 46 der Richtlinie 95/46/EG gestützt werden, indem die zum Schutz der personenbezogenen Daten geeigneten technischen und organisatorischen Maßnahmen bereits „zum Zeitpunkt der Planung des Verarbeitungssystems“ getroffen werden müssen (Scholz, in: Simitis, Kommentar zum BDSG, 7. Aufl. 2011, § 3a Rn. 17).

b) Anliegen des Richtliniengebers in der Richtlinie 2002/58/EG

Der Grundsatz der Datensparsamkeit hat über den Anwendungsbereich der Richtlinie 95/46/EG hinaus Bedeutung. Nach Erwägungsgrund 9 der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation sollen die Mitgliedstaaten bei der Einführung und Weiterentwicklung von neuen Technologien zusammenarbeiten und als Ziele insbesondere die Beschränkung der Verarbeitung personenbezogener Daten auf das erforderliche Mindestmaß und die Verwendung anonymer oder pseudonymer Daten berücksichtigen. Die Ziele, möglichst anonyme oder pseudonyme Daten zu verarbeiten und beim Design der Technik und bei den Verarbeitungsprozessen im Vorwege Lösungen zu entwickeln, um auf einen Personenbezug weitestgehend zu verzichten, entsprechen also gerade dem Anliegen des europäischen Richtliniengebers. Solche Lösungen sollen Gegenstand der Vollharmonisierung des Datenschutzes auf europäischer Ebene sein.

c) Konkretisierung des Drittwirkungsgrundsatzes auf europäischer Ebene

Weiterhin muss die Antragstellerin Art. 8 Abs. 1 und 2 der Charta der Grundrechte der EU beachten. Demnach hat jede Person das Recht auf Schutz der sie betreffenden personenbe-

zogenen Daten. Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. § 13 Abs. 6 TMG bildet eine Konkretisierung dieser datenschutzrechtlichen Grundsätze, was im Wege der mittelbaren Drittwirkung von Grundrechten Berücksichtigung finden muss. Das europäische Datenschutzrecht erfasst nach den gerichtlichen Entscheidungen des EuGH auch privatrechtliche Sachverhalte, bei denen keine staatlichen Organe beteiligt sind: In einem Fall hatte eine Privatperson personenbezogene Daten von 18 Arbeitskollegen ohne deren Einwilligung ins Internet gestellt (EuGH, Urteil vom 6. 11. 2003 - C-101/01 – Lindqvist). In einem anderen Fall forderte ein Verband zur Geltendmachung zustehender Urheberrechte von einem Internetanbieter die Herausgabe von Benutzerdaten (EuGH, Urteil vom 29. 1. 2008 - C-275/06 - Promusicae). Der EuGH hat dabei das Datenschutzgrundrecht als europarechtlichen Maßstab für die Beurteilung der entsprechenden Vorabentscheidungsverfahren angewandt. Dies erfolgte letztlich auch deshalb, weil das Datenschutzgrundrecht zur Interpretation der Richtlinie 95/46/EG herangezogen wurde und die Richtlinie private Datenverarbeitung ebenso erfasst wie staatliche (Britz, Das Grundrecht auf Datenschutz in Art. 8 der Grundrechtecharta, S. 13 f.; abrufbar unter http://www.datenschutz. hessen.de/download. php?download_ID = 188). Im Fall „Lindqvist“ entschied der EuGH, dass die von den Mitgliedstaaten zur Gewährleistung des Schutzes personenbezogener Daten getroffenen Maßnahmen sowohl mit den Bestimmungen der Richtlinie 95/46/EG als auch mit deren Ziel im Einklang stehen müssen, ein Gleichgewicht zwischen dem freien Verkehr personenbezogener Daten und dem Schutz der Privatsphäre zu wahren. Aufgrund dessen entfaltet Art. 8 der Grundrechtecharta über die in ihm enthaltene Schutzpflicht mittelbare Drittwirkung (Streinz/Michl, EuZW 2011, 384, 387). Somit entsteht für nichtöffentliche Stellen eine privatrechtsbindende Wirkung, die sich bei organisatorischen Vorkehrungen zum Datenschutz entfaltet. Der Schutz durch Art. 8 der Grundrechtecharta ist somit bei der Beurteilung der Frage heranzuziehen, welche Maßnahmen der Datensparsamkeit und welche Verarbeitungsformen, wie etwa eine anonyme oder pseudonyme Verarbeitung, zur Wahrung der allgemeinen Persönlichkeitsrechte der Nutzer zu veranlassen sind. § 13 Abs. 6 TMG enthält hierfür konkrete Vorgaben.

d) Zumutbarkeit der Zulassung einer pseudonymen Nutzung

Der Antragstellerin ist die Zulassung einer pseudonymen Nutzung nach Maßgabe von § 13 Abs. 6 TMG technisch möglich und zumutbar. Ergänzend zu den Ausführungen in der Anordnung der Antragsgegnerin vom 14. Dezember 2012 soll nochmals ausgeführt werden, dass technische Maßnahmen zur zukünftigen Unterbindung von z.B. urheber- oder strafrechtlichen Verhaltensweisen von Nutzern für die Antragstellerin auch dann möglich sind, wenn die Nutzer unter Pseudonym agieren. Das Pseudonym ist in diesem Fall bereits ein Identifikator, um etwaigem Missbrauch des Diensteangebots entgegen zu wirken. Damit sind auch sämtliche Behauptungen der Antragstellerin nicht stichhaltig, wonach bei Verwendung von Pseudonymen unkalkulierbare Haftungsrisiken entstehen würden. Eine Verarbeitung von Echtdaten ist z.B. nicht erforderlich um festzustellen, von welchem Accountinhaber rechtswidrige Eintragungen vorgenommen wurden. Maßnahmen, um einem entsprechenden Missbrauch eines Diensteangebots entgegen zu wirken, könnten unter Ermittlung des Pseudonyms ergriffen werden.

Weiterhin besteht für die Antragstellerin die zumutbare Möglichkeit, eine Nutzung des Diensteangebots durch eine Identifikation mit dem elektronischen Personalausweis durchzu-

führen. Personalausweisinhaber können ihre Identität gegenüber öffentlichen und nichtöffentlichen Stellen elektronisch nachweisen. Der Personalausweis besitzt die Funktion, eine Identifizierung via Pseudonym zuzulassen, indem ein dienste- und kartenspezifisches Kennzeichen auslesbar ist, § 18 Abs. 3 Nr. 3 Personalausweisgesetz (PAuswG). Diensteanbieter erhalten unter den Voraussetzungen des § 21 Abs. 2 PAuswG auf schriftlichen Antrag die Berechtigung, die für die Wahrnehmung ihrer Aufgaben oder Geschäftszwecke erforderlichen Daten im Wege des elektronischen Identitätsnachweises beim Inhaber des Personalausweises mittels eines Berechtigungszertifikats anzufragen. Der Antragstellerin ist es zumutbar, beim Bundesverwaltungsamt nach § 28 Abs. 1 der Personalausweisverordnung (PAuswVO) einen Antrag auf Ausstellung einer solchen Berechtigung zu stellen. Bei alleiniger Abrufberechtigung für das dienste- und kartenspezifische Kennzeichen wird im Chip des Personalausweises ein Pseudonym generiert und einem bestimmten Ausweisinhaber zugewiesen. Auf diese Weise ist ein datensparsamer Umgang mit personenbezogenen Daten gewährleistet.

Eine Zusendung von Kopien von Personalausweisen zwecks Kontoentsperrung kann die Antragstellerin hingegen nicht verlangen. Die Erhebung der auf dem Personalausweis aufgedruckten Daten ist nicht erforderlich. Dies gilt in besonderer Weise für das Lichtbild und die Zugangsnummer, die nur dem Ausweisinhaber bekannt sein soll, durch ein Kopieren jedoch in Umlauf geraten kann. Selbst das Bundesministerium des Innern fordert, soweit eine Ausweiskopie ausnahmsweise zulässig sein sollte, dass die Daten erhebende Stelle die Betroffenen auf die Notwendigkeit einer Schwärzung hinweisen muss (Anlage Ast 8). Unabhängig von der Unzulässigkeit einer Personalausweiskopie im vorliegenden Fall nimmt die Antragstellerin auch keine solche Belehrung gegenüber den Nutzern vor.

4. Ordnungsgemäße Interessenabwägung

Bereits in der Anordnung der Antragsgegnerin vom 14. Dezember 2012 wurde zur massiven Behinderung der Meinungsäußerungsfreiheit der Nutzer durch die Selektierung „irrelevanter Beiträge“ durch die Antragstellerin ausgeführt. Vom Schutzbereich der Meinungsfreiheit umfasst sind zum einen Meinungen, das heißt durch das Element der Stellungnahme und des Dafürhaltens geprägte Äußerungen. Sie fallen stets in den Schutzbereich von Art. 5 Abs. 1 Satz 1 GG, ohne dass es dabei darauf ankäme, ob sie sich als wahr oder unwahr erweisen, ob sie begründet oder grundlos, emotional oder rational sind, oder ob sie als wertvoll oder wertlos, gefährlich oder harmlos eingeschätzt werden (BVerfGE 90, 241, 247; 124, 300, 320). Sie verlieren diesen Schutz auch dann nicht, wenn sie scharf und überzogen geäußert werden (BVerfGE 61, 1, 7 f.; 90, 241, 247; 93, 266, 289). Wer damit rechnen muss, von der Antragsgegnerin als „Troll“ identifiziert zu werden (Schreiben der Antragstellerin vom 6. Dezember 2012, S. 6 f. – Anlage Ast 4) und dessen Meinungskundgabe somit über Facebook gesteuert, zugelassen oder erlaubt wird, wird an der Ausübung seiner Meinungsäußerungsfreiheit massiv gehindert. Dies stellt auch einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung dar, wenn die Meinungskundgabe stets von einer Registrierung mit Echtdaten abhängig gemacht wird.

Die anonyme Nutzung ist dem Internet immanent. Der BGH hat in seiner Entscheidung zu Lehrerbewertungsportalen ausgeführt, dass entsprechende Regelungen zur Wahrung der Anonymität auch in den Vorschriften des TMG zu finden sind. Eine Beschränkung der Meinungsäußerungsfreiheit auf Äußerungen, die einem bestimmten Individuum zugeordnet wer-

den können, ist nach den Darlegungen des BGH mit Art. 5 Abs. 1 GG nicht vereinbar (BGH Urteil vom 23.06.2009 - VI ZR 196/08, BGH MMR 2009, 608, 612). „Die Verpflichtung, sich namentlich zu einer bestimmten Meinung zu bekennen, würde nicht nur im schulischen Bereich, um den es im Streitfall geht, die Gefahr begründen, dass der Einzelne aus Furcht vor Repressalien oder sonstigen negativen Auswirkungen sich dahingehend entscheidet, seine Meinung nicht zu äußern. Dieser Gefahr der Selbstzensur soll durch das Grundrecht auf freie Meinungsäußerung entgegengewirkt werden“ (BGH Urteil vom 23.6.2009 - VI ZR 196/08; Ballhausen/Roggenkamp, K&R 2008, 403, 406; OLG Hamm, Beschluss vom 03.08.2011, I 3 U 196/10).

Die Meinungsäußerungsfreiheit der Nutzer wird durch Art. 11 Abs. 1 der Grundrechtecharta geschützt. Hiernach hat jede Person das Recht auf freie Meinungsäußerung. Dieses Recht schließt die Meinungsfreiheit und die Freiheit ein, Informationen und Ideen ohne behördliche Eingriffe und ohne Rücksicht auf Staatsgrenzen zu empfangen und weiterzugeben. § 13 Abs. 6 TMG bildet insofern eine europarechtliche Konkretisierung der Gewährleistung, ohne Zwang eine bestimmte Meinung äußern zu können. Der Äußernde muss seine Meinung unter Verwendung eines Pseudonyms tätigen können, ohne fürchten zu müssen, von der Antragstellerin als Person mit „irrelevanten“ Beiträgen von der Kommunikation ausgeschlossen zu werden. Diese grundrechtliche Gewährleitung muss zwischen der Antragstellerin und den Nutzern im Wege der mittelbaren Drittwirkung von Grundrechten beachtet werden.

Die wettbewerbliche Betätigungsfreiheit der Antragstellerin muss hier zurücktreten. Nach Art. 16 der Grundrechtscharta wird die unternehmerische Freiheit nach dem Gemeinschaftsrecht und den einzelstaatlichen Rechtsvorschriften und Gepflogenheiten anerkannt. Nach Art. 52 Abs. 1 Satz 2 der Grundrechtecharta dürfen unter Wahrung des Grundsatzes der Verhältnismäßigkeit Einschränkungen nur dann vorgenommen werden, wenn sie notwendig sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen. Die Meinungsäußerungsfreiheit der Nutzer sowie das ihnen zustehende allgemeine Persönlichkeitsrecht verdienen gegenüber der wettbewerblichen Betätigungsfreiheit der Antragstellerin Vorrang. Gerade kritische Meinungsäußerungen können von den Nutzern nur dann unter den angelegten Accounts verbreitet werden, wenn diese sicher sein können, dass keine Zensur durch die Antragstellerin erfolgt. Dabei muss die Freiheit bestehen, Meinungsäußerungen unter Nutzung eines Pseudonyms in die Kommunikation mit anderen Nutzern einzubringen. Nutzer müssen dabei die Möglichkeit erhalten, gegenüber anderen Nutzern per Pseudonym aufzutreten. Missstände müssen dann offen diskutiert werden können, ohne dass die Nutzer mit Nachteilen rechnen müssen (OLG Hamm, Beschluss vom 03.08.2011, I 3 U 196/10). Die Antragstellerin hat kein Recht in diese Kommunikation aktiv einzugreifen, indem sie Kontensperrungen vornimmt und Äußerungen unter Pseudonym unmöglich macht. Weiterhin hat die Antragstellerin nicht die Befugnis, eine Kommunikation der Nutzer von vornherein ohne Ausnahme unter Offenbarung ihrer Identität zu fordern. Die Ermöglichung einer Kommunikation unter Pseudonym entspricht auch den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen. Dabei ist die Meinungsfreiheit nicht auf die Äußerung von Meinungen beschränkt, sondern schließt nach Art. 10 Abs. 1 Satz 2 der EMRK und Art. 11 Abs. 1 Satz 1 der Grundrechtecharta im Sinne einer Kommunikationsfreiheit ausdrücklich die Freiheit zum Empfang und zur Mitteilung von Nachrichten oder Ideen ein. Dieses Recht wird durch eine Kontensperrung massiv behindert. Der EGMR betont in ständiger Rechtsprechung, dass die Freiheit der Meinungsäußerung nicht nur für Informationen oder Ideen gilt, die Zustimmung erfah-

ren oder die als harmlos oder unerheblich betrachtet werden, sondern auch für sämtliche Informationen und Ideen, die den Staat oder einen Bereich der Bevölkerung beleidigen, aus der Fassung bringen oder stören (EuGH, Schlussantrag des Generalanwalts v. 08.05.2008, Rechtssache C-73/07).

Eine Missbrauchskontrolle bleibt der Antragstellerin möglich, wenn einzelne Nutzer davon Gebrauch machen, auf dem Facebookportal unter Pseudonym aufzutreten. Erhält die Antragstellerin Kenntnis davon, dass z.B. ein strafrechtlich relevantes Verhalten von einzelnen Nutzern vorliegt, so wäre der jeweilige Verursacher über das Pseudonym zu ermitteln und Maßnahmen gegen einen Missbrauch können ergriffen werden. Das Angebot an die Nutzer, eine Registrierung unter Pseudonym vorzunehmen, ist der Antragstellerin zumutbar, zumal über die Funktion des elektronischen Personalausweises neue Möglichkeiten einer Identifizierung möglich sind. Der Gesetzgeber hat die Möglichkeit einer Verwendung des elektronischen Identitätsnachweises z.B. auch für Kreditinstitute geregelt, wodurch ein besonderes sparsamer Umgang mit personenbezogenen Daten erfolgen kann, vgl. §§ 6 Abs. 2 Nr. 2 Satz 1 c), 8 Abs. 1 Satz 6 PAuswG.

Weiterhin liegt ein Verstoß gegen Art. 8 Abs. 1 und 2 der Grundrechtecharta vor. Nach Art. 8 Abs. 2 Satz 2 der Grundrechtscharta dürfen personenbezogene Daten nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten Grundlage verarbeitet werden. Eine Einwilligung der Nutzer liegt nicht vor, da diese voraussetzen würde, dass die Nutzer eine freie Entscheidung über die Verwendung ihrer Echtdaten bei der Registrierung fällen können. Dies ist durch den von der Antragstellerin ausgeübten Zwang auf die Nutzer, sich mit Echtdaten zu registrieren, nicht gegeben. Insofern haben die betroffenen Nutzer keine Einwilligung nach Maßgabe von Art. 7 a) der Richtlinie 95/46/EG, Art. 8 Abs. 2 Satz 1 der Grundrechtscharta erteilt. Die Eingabe der Echtdaten kann auch nicht auf eine gesetzliche Grundlage gestützt werden. Die Verarbeitung der Daten ist nicht für die Erfüllung eines Vertrags erforderlich, Art. 7 b) der Richtlinie 95/46/EG. Es bestehen auf Seiten der Antragstellerin keine legitimen Zwecke, ohne Ausnahme den Gebrauch von Pseudonymen zu verbieten. Dabei ist auch zu berücksichtigen, dass keine Vertragspflichten der Nutzer gegenüber der Antragstellerin bestehen, die eine Übermittlung personenbezogener Daten zwingend notwendig macht, wie dies etwa bei einem Kaufvertrag bezüglich der Angabe der Rechnungsadresse denkbar wäre. Eine wie von der Antragstellerin vorgetragene „Klarnamenpolitik“ muss im Rahmen der ihr zustehenden wirtschaftlichen Betätigungsfreiheit hinter dem Schutz der allgemeinen Persönlichkeitsrechte der Nutzer zurückstehen.

Vor diesem Hintergrund ist die Anordnung der sofortigen Vollziehung bezüglich der Entsperrung von Nutzerkonten rechtmäßig. Es besteht ein hohes öffentliches Interesse an der Ermöglichung eines freien Meinungsaustausches und der Wahrung der Privatsphäre. Eine Kommunikation, die Nutzer gesperrter Konten bisher über das Portal der Antragstellerin geführt haben, ist diesen nicht mehr zugänglich. Hierdurch wird Meinungsbildung und -äußerung gezielt verhindert. Ein Zwang zur Offenbarung der Identität beschränkt in unzulässiger Weise die allgemeinen Persönlichkeitsrechte der Nutzer. Eine Zensur von Meinungen durch die Antragstellerin verstößt eklatant gegen die Meinungsäußerungsfreiheit. Da die Antragstellerin nun zu einer Sperrung von Nutzerkonten übergegangen ist, um die Herausgabe von Echtdaten und ungeschwärzten Kopien von Personalausweiskopien auf rechtswidrige Weise zu er-

zwingen und den Nutzern keine Wahlmöglichkeiten eingeräumt werden, um auf eigene Kommunikationsinhalte zurückzugreifen, besteht ein öffentliches Vollzugsinteresse.

Sollte nach Auffassung des Gerichts weiterer Erläuterungsbedarf bestehen, bitten wir höflich um einen Hinweis. Für Rückfragen stehen wir zur Verfügung.

gez. im Auftrag

Dr. Sven Polenz