



Verwaltungsgericht Hamburg
Beschluss

In der Verwaltungsrechtssache

F. Ireland Limited

- Antragstellerin -

Prozessbevollmächtigte:

g e g e n

die Freie und Hansestadt Hamburg,
vertreten durch den Hamburgischen Beauftragten für Daten-
schutz und Informationsfreiheit,
Klosterwall 6,
20095 Hamburg,

- Antragsgegnerin -

hat das Verwaltungsgericht Hamburg, Kammer 15, am 3. März 2016 durch

...

beschlossen:

1. Die aufschiebende Wirkung des Widerspruchs der Antragstellerin gegen die Anordnung Ziffer I.1. des Bescheids vom 24. Juli 2015 wird wiederhergestellt.
2. Die Kosten des Verfahrens hat die Antragsgegnerin zu tragen.
3. Der Wert des Streitgegenstands wird auf 2.500,00 € festgesetzt.

Rechtsmittelbelehrung:

Gegen diesen Beschluss steht den Beteiligten und sonst von der Entscheidung Betroffenen die Beschwerde an das Oberverwaltungsgericht zu. Sie ist innerhalb von zwei Wochen nach Bekanntgabe des Beschlusses schriftlich oder durch ein mit einer qualifizierten elektronischen Signatur versehenes und elektronisch übermitteltes Dokument (§ 55a der Verwaltungsgerichtsordnung – VwGO – i.V.m. der Verordnung über den elektronischen Rechtsverkehr in Hamburg vom 28. Januar 2008 in der jeweils geltenden Fassung) beim Verwaltungsgericht Hamburg, Lübeckertordamm 4, 20099 Hamburg, einzulegen.

Die Beschwerdefrist wird auch gewahrt, wenn die Beschwerde innerhalb der Frist beim Hamburgischen Oberverwaltungsgericht, Lübeckertordamm 4, 20099 Hamburg, schriftlich oder in elektronischer Form (s.o.) eingeht.

Die Beschwerde ist innerhalb eines Monats nach Bekanntgabe der Entscheidung zu begründen. Die Begründung ist, sofern sie nicht bereits mit der Beschwerde vorgelegt worden ist, bei dem Hamburgischen Oberverwaltungsgericht, Lübeckertordamm 4, 20099 Hamburg, schriftlich oder in elektronischer Form (s.o.) einzureichen. Sie muss einen bestimmten Antrag enthalten, die Gründe darlegen, aus denen die Entscheidung abzuändern ist oder aufzuheben ist, und sich mit der angefochtenen Entscheidung auseinandersetzen.

Eine Beschwerde in Streitigkeiten über Kosten, Gebühren und Auslagen ist nur zulässig, wenn der Wert des Beschwerdegegenstandes 200,00 EUR übersteigt.

Der Beschwerde sowie allen Schriftsätzen sollen – sofern sie nicht in elektronischer Form eingereicht werden – Abschriften für die Beteiligten beigelegt werden.

Vor dem Oberverwaltungsgericht müssen sich die Beteiligten, außer im Prozesskostenhilfverfahren, durch Prozessbevollmächtigte vertreten lassen. Dies gilt auch für Prozesshandlungen, durch die ein Verfahren vor dem Oberverwaltungsgericht eingeleitet wird. Als Bevollmächtigte sind Rechtsanwälte oder Rechtslehrer an einer der in § 67 Abs. 2 Satz 1 VwGO genannten Hochschulen mit Befähigung zum Richteramt zugelassen. Ferner sind die in § 67 Abs. 2 Satz 2 Nr. 3 bis 7 VwGO bezeichneten Personen und Organisationen als Bevollmächtigte zugelassen. Ergänzend wird wegen der weiteren Einzelheiten auf § 67 Abs. 2 Satz 3, Abs. 4 und Abs. 5 VwGO verwiesen.

Hinsichtlich der Festsetzung des Streitwertes steht den Beteiligten die Beschwerde an das Hamburgische Oberverwaltungsgericht zu. Die Streitwertbeschwerde ist schriftlich oder zur Niederschrift des Urkundsbeamten der Geschäftsstelle oder in elektronischer Form (s.o.) beim Verwaltungsgericht Hamburg, Lübeckertordamm 4, 20099 Hamburg, einzulegen.

Sie ist spätestens innerhalb von sechs Monaten, nachdem die Entscheidung in der Hauptsache Rechtskraft erlangt hat, einzulegen.

Soweit die Beschwerde gegen die Streitwertfestsetzung nicht durch das Verwaltungsgericht zugelassen worden ist, ist eine Beschwerde gegen die Streitwertfestsetzung nur gegeben, wenn der Wert des Beschwerdegegenstandes 200,00 EUR übersteigt.

Gründe:

I.

Die Antragstellerin begehrt vorläufigen Rechtsschutz gegen eine datenschutzrechtliche Anordnung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (im Folgenden: Datenschutzbeauftragter).

Die Antragstellerin, die Facebook Ireland Limited, ist eine Gesellschaft irischen Rechts. Sie bildet den Hauptgeschäftssitz des F.-Konzerns außerhalb Nordamerikas. Gesellschaftsrechtlich wird die Antragstellerin durch die F., Inc. mit Sitz in den Vereinigten Staaten kontrolliert. Die F., Inc. betreibt die technische Plattform des F.-Netzwerks. Übereinstimmend gehen die Beteiligten davon aus, dass die Antragstellerin für die Verarbeitung der personenbezogenen Daten unter anderem der europäischen Nutzer von F. verantwortlich ist. Zwischen der Antragstellerin und der F., Inc. besteht seit 2010 ein Data Transfer and Processing Agreement. Die Vereinbarung trifft Regelungen zu den Umständen, unter denen die F., Inc. für die Antragstellerin Daten verarbeitet. Die Vereinbarung dient nach ihrer Präambel der Einhaltung unter anderem irischer datenschutzrechtlicher Vorschriften und regelt, dass die Antragstellerin für die Verarbeitung personenbezogener Daten aus dem Europäischen Wirtschaftsraum durch die F., Inc. verantwortlich sein soll. Die F., Inc. soll diese Daten im datenschutzrechtlichen Sinne im Auftrag der Antragstellerin verarbeiten.

Die F. Germany GmbH (im Folgenden: F. Germany) wurde 2009 gegründet und hat ihren Sitz in Hamburg. Sie steht im alleinigen Eigentum der F. Global Holdings II, LLC. Die F. Global Holdings II, LLC wird gesellschaftsrechtlich durch die F., Inc. kontrolliert. F. Germany akquiriert Werbeanzeigen für die Antragstellerin und unterstützt die Antragstellerin im Marketing. Gegenstand des Unternehmens ist laut Eintragung im Handelsregister „das Angebot von Anzeigenakquise (die Akquise von Anzeigen) und (die Bereitstellung) von Marketingfunktionen für die Internetseite eines sozialen Netzwerks.“ Nach den Angaben der Antragstellerin, die der Datenschutzbeauftragte nicht infrage stellt, unterhält F. Germany Beziehungen zu Werbeagenturen, Kunden und Partnern der Antragstellerin in Deutschland. Sie arbeitet im Bereich der Einrichtung und Auslieferung von Werbeangeboten der Antragstellerin. Angestellte von F. Germany sind zudem im Bereich der Öffentlich-

keitsarbeit sowie der politischen Interessenvertretung tätig. Im Mai 2015 arbeiteten für F. Germany 58 Mitarbeiter. Übereinstimmend gehen die Beteiligten davon aus, F. Germany sei in begrenztem Umfang als Auftragsdatenverarbeiterin für die Antragstellerin tätig. Mit Schreiben vom 19. Mai 2015 teilte F. Germany dem Datenschutzbeauftragten mit: Die Antragstellerin [die F. Ireland Limited] kontrolliere die Daten der europäischen Nutzer. F. Germany treffe keine Entscheidungen über die Verwendung dieser Daten. In begrenztem Umfang habe sie Zugang zu den Daten von Kunden. Dabei handle es sich insbesondere um die Daten von Werbekunden, die F. Germany betreue. Nur solche Daten verarbeite F. Germany. Dabei sei sie im Auftrag und nach Weisung der Antragstellerin tätig.

In den Nutzungsbedingungen des Netzwerks F. („Erklärung der Rechte und Pflichten“) heißt es unter anderem:

„4. Registrierung und Kontosicherheit

F.-Nutzer geben ihre wahren Namen und Daten an, und wir benötigen deine Hilfe, damit dies so bleibt. Nachfolgend werden einige Verpflichtungen aufgeführt, die du uns gegenüber bezüglich der Registrierung und der Wahrung der Sicherheit deines Kontos eingehst:

1. Du wirst keine falschen persönlichen Informationen auf F. bereitstellen [...].
[...]
7. Du wirst dafür sorgen, dass deine Kontaktinformationen stets korrekt sind und sich auf dem neuesten Stand befinden.
[...]
10. Wenn du einen Nutzernamen bzw. eine ähnliche Kennung für dein Konto oder deine Seite auswählst, behalten wir uns das Recht vor, diese/n zu entfernen oder zu widerrufen, sollten wir dies als notwendig erachten (zum Beispiel, wenn ein Markeninhaber eine Beschwerde über einen Nutzernamen einreicht, welcher nicht in engem Bezug zum tatsächlichen Namen eines Nutzers steht).
[...]
15. Streitfälle
 1. Du wirst jedweden Anspruch [...], den du uns gegenüber hast und der sich aus dieser Erklärung oder in Verbindung mit dieser bzw. mit F. ergibt, ausschließlich vor dem für den nördlichen Bezirk von Kalifornien zuständigen US-Bezirksgericht oder vor einem Staatsgericht in San Mateo County klären bzw. klären lassen, und du stimmst zu, dass du dich bei einem Prozess hinsichtlich aller derartigen Ansprüche der personenbezogenen Gerichtsbarkeit dieser Gerichte unterwirfst. Diese Erklärung sowie alle Ansprüche, die möglicherweise zwischen dir

und uns entstehen, unterliegen den Gesetzen des Bundesstaates Kalifornien, und zwar unter Ausschluss der Bestimmungen des internationalen Privatrechts.

[...]

16. Besondere Bestimmungen für Nutzer außerhalb der USA

[...]

3. Bestimmte Sonderbedingungen, die nur für deutsche Nutzer gelten, findest du hier. [Hyperlink]

[...]

18. Sonstiges

1. Wenn du in den USA oder Kanada ortsansässig ist oder dort einen Hauptgeschäftssitz hast, stellt diese Erklärung einer Vereinbarung zwischen dir und F., Inc. dar. Andernfalls stellt diese Erklärung eine Vereinbarung zwischen dir und F. Ireland Limited dar. Die Begriffe „uns“, „wir“ und „unser/e“ verweisen jeweils entweder auf F., Inc. oder F. Ireland Limited.“

In den Sonderbedingungen, die gemäß Ziffer 16.3 der „Erklärung der Rechte und Pflichten“ für deutsche Nutzer gelten, heißt es unter anderem:

„5. Ziffer 15.1 wird ersetzt durch: Diese Erklärung unterliegt deutschem Recht.“

Am 2. Dezember 2014 wandte sich der Datenschutzbeauftragte per E-Mail an die Antragstellerin. Sie möge sicherstellen, dass Nutzerinnen und Nutzer zum Zwecke der Feststellung ihrer Identität nicht aufgefordert würden, Scans amtlicher Ausweisdokumente zu übersenden. Er wies dabei auf das Recht der Nutzerinnen und Nutzer von Telemediendiensten auf pseudonyme bzw. anonyme Nutzung aus § 13 Abs. 6 TMG hin. Soweit F. eine Identitätsfeststellung rechtlich fordern könne und dies erforderlich sei, könne dies gemäß § 18 PAuswG / § 18 PassG im Wege der elektronischen Identitätsfeststellung erfolgen.

Anlass des streitgegenständlichen Verwaltungsverfahrens gegen die Antragstellerin war die Eingabe einer Nutzerin von F.. Die Betroffene ist als ... tätig und seit mehreren Jahren Nutzerin von F.. Ursprünglich nutzte sie F. unter Verwendung ihres bürgerlichen Namens. Sie änderte dies später in Pseudonyme wie „...“. Hiermit bezweckte sie ihren Angaben zufolge, eine Vermischung ihrer beruflichen Tätigkeit und ihrer privaten Aktivitäten auf F. zu vermeiden. Sie wolle nicht auf ihrem privaten F.-Konto von ... angeschrieben werden.

Nach Zweifeln an der Authentizität des Profils der Betroffenen sperrte die Antragstellerin Anfang Juni 2015 den Zugang der Betroffenen zu ihrem Konto. Im weiteren Verlauf übersandte die Betroffene der Antragstellerin Abbildungen verschiedener Dokumente zur Klärung ihrer Identität. Diese ließ die Antragstellerin nicht genügen.

Mit E-Mail vom 15. Juni 2015 bat die Antragstellerin die Betroffene, ein Foto zu übersenden, auf dem sie und ihr amtlicher Ausweis zu erkennen seien.

Am 17. Juni 2015 wandte sich die Betroffene an den Datenschutzbeauftragten.

Mit E-Mail vom 24. Juni 2015 bat der Datenschutzbeauftragte die Antragstellerin, zum Fall der Betroffenen Stellung zu nehmen. F. verstoße weiterhin gegen das gesetzliche Verbot der automatisierten Erhebung von Daten aus amtlichen Ausweisen.

Am 8. Juli 2015 antwortete die Antragstellerin dem Datenschutzbeauftragten, dass die Nutzer von F. durch die „Erklärung der Rechte und Pflichten“ verpflichtet seien, ihre wahren Namen und Daten anzugeben. Für alle Nutzer von F. in Deutschland sei die Antragstellerin der Anbieter von „Diensten der Informationsgesellschaft“ im Sinne der Richtlinie 2000/31/EG (sog. E-Commerce-Richtlinie) und die „für die Verarbeitung Verantwortliche“ im Sinne der Richtlinie 95/46/EG (sog. Datenschutzrichtlinie). Sie, die Antragstellerin, handle in Übereinstimmung mit dem anzuwendenden irischen Datenschutzrecht. F. biete Nutzern, die ihre Identität zu verifizieren hätten, eine Vielzahl von Möglichkeiten. Die Betroffene habe scheinbar nicht ihren wahren Namen als Profilnamen verwendet. Nach entsprechender Überprüfung habe F. das Profil der Betroffenen reaktiviert, aber ihren Profilnamen in ihren wahren Namen verändert.

In der Folge erhielt die Betroffene wieder Benachrichtigungen von F.. Beim Versuch, sich in ihr Konto einzuloggen, bat F. die Betroffene, der Änderung ihres Namens in ihren vollen Vor- und Nachnamen zuzustimmen. Dies tat die Betroffene nicht. Einen Zugriff auf ihr Nutzerkonto hat sie vor diesem Hintergrund bis heute nicht. Das Profil der Betroffenen ist aufgrund der Sperrung für andere Nutzer derzeit nicht sichtbar. Vor- und Nachname der Betroffenen werden aber in bestimmten Zusammenhängen anderen Nutzern angezeigt.

Mit Bescheid vom 24. Juli 2015 verpflichtete der Datenschutzbeauftragte die Antragstellerin, die Änderung des Namens der Betroffenen zurückzunehmen und der Betroffenen die uneingeschränkte Nutzung ihres F.-Kontos unter ihrem früheren Pseudonym zu ermöglichen (Ziffer I.1 des Bescheids) und ordnete insoweit die sofortige Vollziehung an (Ziffer I.3 des Bescheids). Darüber hinaus untersagte der Datenschutzbeauftragte der Antragstellerin unter Berufung auf personalausweis- und passrechtliche Bestimmungen, zur Durchsetzung ihres Klarnamenprinzips von Nutzern Vervielfältigungen amtlicher Ausweisdokumente zu verlangen und zu speichern (Ziffer I.2 des Bescheids). Zur Begründung der Verpflichtung der Antragstellerin, der Betroffenen die uneingeschränkte pseudonyme Nutzung ihres F.-Kontos zu ermöglichen, berief sich der Datenschutzbeauftragte auf §§ 13 Abs. 6, 12 Abs. 1 TMG. Auf die Antragstellerin sei deutsches Datenschutzrecht einschließlich der datenschutzrechtlichen Vorschriften des Telemediengesetzes anzuwenden. Auf die Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeit einer Niederlassung des für die Verarbeitung Verantwortlichen ausgeübt werde, sei das jeweilige nationale Datenschutzrecht des Sitzstaates der Niederlassung anzuwenden. Unter Berücksichtigung der Rechtsprechung des Europäischen Gerichtshofs sei § 1 Abs. 5 Satz 1 Halbsatz 2 BDSG dahingehend auszulegen, dass nationales Datenschutzrecht anzuwenden sei, sofern eine in einem anderen Mitgliedsstaat der Europäischen Union belegene verantwortliche Stelle bei der Datenverarbeitung durch eine Niederlassung im Inland Unterstützung erhalte. Die Antragstellerin werde bei der Datenverarbeitung durch die in Hamburg ansässige F. Germany unterstützt. Deshalb sei er, der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, zum Erlass der Anordnung sachlich und örtlich zuständig. In materieller Hinsicht verstoße die Antragstellerin gegen § 13 Abs. 6 TMG, indem sie der Betroffenen die pseudonyme Nutzung von F. nicht ermögliche. Die pseudonyme Nutzung sei technisch möglich und der Antragstellerin auch zumutbar. Für die Umbenennung des Kontos der Betroffenen und die damit verbundene Übermittlung des Namens der Betroffenen gegenüber anderen Nutzerinnen und Nutzern von F. fehle es der Antragstellerin an der nach § 12 Abs. 1, Abs. 2 TMG erforderlichen rechtlichen Grundlage. Im Interesse der Betroffenen sei auch die sofortige Vollziehung der Verpflichtung der Antragstellerin gemäß § 80 Abs. 2 Satz 1 Nr. 4 Var. 2 VwGO anzuordnen. Der Betroffenen sei es nicht zuzumuten, dass ihr der Zugriff auf das unter ihrem Pseudonym geführte Konto bis zur Unanfechtbarkeit des Bescheids verwehrt werde. Durch den Zwang, ihr Nutzerkonto nach außen hin unter ihrem Klarnamen führen zu müssen, werde die Betroffene in ihrem Recht auf informationelle Selbstbestimmung verletzt.

Mit Schriftsatz vom 4. August 2015 legte die Antragstellerin hiergegen Widerspruch ein.

Am 6. August 2015 hat die Antragstellerin bei Gericht vorläufigen Rechtsschutz beantragt. Zur Begründung macht die Antragstellerin unter anderem geltend: Der Hamburgische Datenschutzbeauftragte sei für den Erlass der streitigen Anordnung weder international noch örtlich zuständig. Der Datenschutzbeauftragte sei zwar befugt, den vorliegenden Fall auf der Grundlage deutschen Verfahrensrechts zu untersuchen. Für verbindliche Anordnungen gegenüber der Antragstellerin seien aber die irischen Datenschutzbehörden international zuständig. Denn auch in der Sache sei irisches Datenschutzrecht anzuwenden. Die Zuständigkeit nationaler Datenschutzbehörden sei unter Berücksichtigung der Richtlinie 95/46/EG zu bestimmen. Zuständig sei die Behörde desjenigen Mitgliedsstaats, dessen Datenschutzrecht anwendbar sei. Eine internationale Zuständigkeit deutscher Datenschutzbehörden unterstellt, sei der Datenschutzbeauftragte nicht örtlich zuständig. Die Antragstellerin sitze nicht in seinem Bezirk und die Betroffene habe ihren gewöhnlichen Aufenthalt in Köln. In materieller Hinsicht könne sich der Datenschutzbeauftragte nicht auf § 13 Abs. 6 TMG berufen. Auf die streitige Datenverarbeitung sei gemäß den einschlägigen deutschen und europarechtlichen Bestimmungen allein irisches Recht anzuwenden. Dies gelte auch unter Berücksichtigung der Rechtsprechung des Europäischen Gerichtshofs. Mit dem anzuwendenden irischen Datenschutzrecht stehe das Klarnamenprinzip im Einklang. Die streitige Verarbeitung personenbezogener Daten finde im Sinne des Art. 4 Abs. 1 lit. a Richtlinie 95/46/EG ausschließlich im Rahmen der Tätigkeit ihrer, der Antragstellerin, Niederlassung in Dublin statt. Eine Anwendung deutschen Datenschutzrechts könne nicht an die Existenz von F. Germany geknüpft werden. F. Germany habe keinen Einfluss auf die Verarbeitung der personenbezogenen Daten der Nutzer der Antragstellerin. Die alleinige Anwendbarkeit irischen Datenschutzrechts auf ihre, der Antragstellerin, Verarbeitung personenbezogener Daten europäischer Nutzer sei nicht Ausdruck eines möglichen „Race to the Bottom“ der Standards des Datenschutzes der Mitgliedsstaaten der EU. Ein effektiver datenschutzrechtlicher Schutz nach den Standards der Richtlinie 95/46/EG bleibe gewährleistet. Gehe man von datenverarbeitenden Niederlassungen der Antragstellerin in mehreren Mitgliedsstaaten aus, sei das anzuwendende Datenschutzrecht das Recht des Mitgliedsstaats derjenigen Niederlassung, die mit der fraglichen Datenverarbeitung am engsten verbunden sei. Dies sei sie, die Antragstellerin, und nicht F. Germany. Dessen ungeachtet verstoße § 13 Abs. 6 TMG gegen Europarecht. Jedenfalls

führe eine unionsrechtskonforme Anwendung dazu, dass das für ihre Nutzer geltende Klarnamenprinzip mit § 13 Abs. 6 TMG vereinbar sei.

Die Antragstellerin beantragt sinngemäß,

die aufschiebende Wirkung ihres Widerspruchs gegen die Anordnung Ziffer I.1. des Bescheids vom 24. Juli 2015 wiederherzustellen.

Aus dem Vorbringen des Datenschutzbeauftragten ergibt sich sein Antrag,

den Antrag abzulehnen.

Er sei zuständig und habe zu Recht deutsches Datenschutzrecht gegenüber der Antragstellerin angewendet. Dies ergebe sich aus einer Anwendung der datenschutzrechtlichen Bestimmungen gemäß der Rechtsprechung des Europäischen Gerichtshofs. Die Tätigkeit einer Niederlassung des für die Datenverarbeitung Verantwortlichen führe bereits dann zur Anwendung der datenschutzrechtlichen Bestimmungen des Mitgliedsstaats der Niederlassung, wenn die Niederlassung den Betrieb des im nationalen Markt angebotenen Dienstes wirtschaftlich rentabel mache und der Dienst im Gegenzug gleichzeitig das Mittel sei, die Tätigkeit der Niederlassung zu ermöglichen. Dies gelte auch für Dienstleister, deren für die Datenverarbeitung verantwortliche Stelle innerhalb der EU belegen sei und die daneben weitere Niederlassungen mit wirtschaftlicher Ausrichtung in anderen Mitgliedsstaaten betrieben. Die Betroffenen seien davor zu schützen, dass im räumlichen Geltungsbereich der Richtlinie 95/46/EG der Mitgliedsstaat mit dem schwächsten Vollzugs- und Umsetzungsniveau am Ende europaweit die Standards für die Umsetzung des Datenschutzes gegenüber global agierenden Datenverarbeitern setze. Seine Zuständigkeit folge aus der Tätigkeit der in Hamburg ansässigen F. Germany. Die Verweigerung pseudonymer Nutzung verstoße gegen § 13 Abs. 6 TMG. Diese Regelung sei europarechtskonform. Seine Anordnung sei auch frei von Ermessensfehlern, insbesondere verhältnismäßig.

II.

Die Kammer hat das Rubrum von Amts wegen geändert. Richtige Antragsgegnerin ist die Freie und Hansestadt Hamburg als Rechtsträgerin des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit. Nur die Freie und Hansestadt ist gemäß § 61 Nr. 1 VwGO in Hamburg fähig, am verwaltungsgerichtlichen Verfahren beteiligt zu sein. Der hamburgische Gesetzgeber hat von der durch § 61 Nr. 3 VwGO eröffneten Möglichkeit, die Beteiligungsfähigkeit von Behörden anzuordnen, keinen Gebrauch gemacht. Aufgrund seiner gemäß § 22 Abs. 1 HmbDSG weitgehend unabhängigen Stellung ist anzunehmen, dass der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit die Freie und Hansestadt unmittelbar vertritt (vgl. für den Bundesbeauftragten: OVG Nordrhein-Westfalen, Beschl. v. 25.3.2009, 5 B 1184/08, juris, Rn. 3).

III.

Der zulässige, insbesondere gemäß § 80 Abs. 5 Satz 1 Var. 2 VwGO statthafte Antrag auf Wiederherstellung der aufschiebenden Wirkung des Widerspruchs der Antragstellerin ist auch begründet. In der Sache überwiegt das Interesse der Antragstellerin, von der sofortigen Vollziehung der streitigen Anordnung des Datenschutzbeauftragten vorläufig verschont zu bleiben, das Interesse der Öffentlichkeit an deren sofortigen Vollziehung. Denn nach summarischer Prüfung unter Berücksichtigung des bisherigen Sach- und Streitstandes dürfte der Widerspruch der Antragstellerin Erfolg haben. Die angefochtene Anordnung des Datenschutzbeauftragten ist voraussichtlich rechtswidrig.

1. Die angegriffene Anordnung ist voraussichtlich materiell rechtswidrig. Mangels Anwendbarkeit materieller deutscher datenschutzrechtlicher Bestimmungen auf die angegriffene Datenverarbeitung vermag insbesondere ein Verstoß gegen § 13 Abs. 6 TMG den Erlass der Anordnung nicht zu rechtfertigen.

Die angegriffene Datenverarbeitung besteht in der Verweigerung der pseudonymen Nutzung des Netzwerks F.. Der Betroffenen wird technisch und gestützt auf entsprechende Nutzungsbedingungen nicht gestattet, das Netzwerk ohne Bekanntgabe ihres (wahren) Vor- und Nachnamens zu nutzen.

a) Der Datenschutzbeauftragte wird die streitige Anordnung nicht aufgrund einer Rechtswahl zwischen der Betroffenen und der Antragstellerin auf deutsche datenschutzrechtliche Bestimmungen stützen können. Dabei kann an dieser Stelle offen bleiben, ob sich die Antragstellerin gegenüber der Betroffenen privatrechtlich wirksam verpflichtet hat, im Nutzungsverhältnis mit der Betroffenen deutsche datenschutzrechtliche Bestimmungen zu beachten (so jedenfalls für privatrechtliche datenschutzrechtliche Bestimmungen wohl LG Berlin, Urt. v. 6.3.2012, 16 O 551/10, juris, Rn. 36 f. und nachfolgend KG Berlin, Urt. v. 24.1.2014, 5 U 42/12, juris, Rn. 141 ff.). Offen bleiben kann ferner, ob die Anwendung deutschen öffentlich-rechtlichen Datenschutzrechtes zur Disposition privatrechtlicher Vertragsparteien steht (dagegen Schleswig-Holsteinisches VG, Beschl. v. 14.2.2013, 8 B 61/12, juris, Rn. 10-12). Eine solche Rechtswahl zwischen Subjekten des Privatrechts vermag eine hoheitliche Eingriffsbefugnis jedenfalls nicht zu begründen.

b) Auch datenschutzrechtliches Kollisionsrecht führt im vorliegenden Fall voraussichtlich nicht zur Anwendung deutscher datenschutzrechtlicher Bestimmungen. Welches Recht auf die streitige Datenverarbeitung anzuwenden ist, bestimmt sich nach § 1 Abs. 5 BDSG in Verbindung mit Art. 4 Richtlinie 95/46/EG [unten aa)]. Die Anwendung deutscher datenschutzrechtlicher Bestimmungen folgt aber weder aus § 1 Abs. 5 Satz 2 BDSG in Verbindung mit Art. 4 Abs. 1 lit. c Richtlinie 95/46/EG [unten bb)] noch aus § 1 Abs. 5 BDSG in Verbindung mit Art. 4 Abs. 1 lit. a Richtlinie 95/46/EG [unten cc)].

aa) Welches nationale Recht auf die streitige Datenverarbeitung anzuwenden ist, ist gemäß § 1 Abs. 5 BDSG und Art. 4 Richtlinie 95/46/EG zu bestimmen. Das soziale Netzwerk F. stellt zwar ein Telemedienangebot im Sinne von § 1 Abs. 1 TMG dar. Mangels spezifischer telemedienrechtlicher Regelungen sind zur Bestimmung des auf Telemedien anzuwendenden Datenschutzrechts aber die allgemeinen datenschutzrechtlichen Kollisionsvorschriften heranzuziehen (vgl. auch Schreibauer, in: Auernhammer, BDSG, 4. Aufl. 2014, Vorbemerkung zu § 11 TMG, Rn. 24, m.w.N.; Plath, in: Plath, BDSG, 1. Aufl. 2013, § 11 TMG, Rn. 20). Zwar unterliegt die geschäftsmäßige Erbringung von Telemedien grundsätzlich dem Recht des Ortes der Niederlassung des Diensteanbieters (Herkunftslandprinzip, vgl. etwa § 3 Abs. 1 TMG; ferner Erwägungsgrund 22 der Richtlinie 2000/31/EG). Gemäß § 3 Abs. 3 Nr. 4 TMG und in Übereinstimmung mit Art. 1 Abs. 5 lit. b Richtlinie 2000/31/EG gilt das Herkunftslandprinzip im Bereich der Telemedien jedoch nicht für die Bestimmung des Rechts, das für den Schutz personenbezogener Daten gilt.

Insoweit gelten die allgemeinen datenschutzrechtlichen Bestimmungen. Der deutsche Gesetzgeber hat das allgemeine datenschutzrechtliche Kollisionsrecht in § 1 Abs. 5 BDSG normiert, der unter anderem der Umsetzung von Art. 4 Richtlinie 95/46/EG dient.

bb) Die Anwendung deutscher datenschutzrechtlicher Bestimmungen folgt nicht aus § 1 Abs. 5 Satz 2 BDSG in Verbindung mit Art. 4 Abs. 1 lit. c Richtlinie 95/46/EG.

Gemäß § 1 Abs. 5 Satz 2 BDSG sind deutsche datenschutzrechtliche Bestimmungen anzuwenden, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt. Unter Berücksichtigung von Art. 4 Abs. 1 lit. c Richtlinie 95/46/EG ist § 1 Abs. 5 Satz 2 BDSG dahingehend auszulegen und anzuwenden, dass eine Anwendung der Vorschrift voraussetzt, dass der für die Datenverarbeitung Verantwortliche im territorialen Geltungsbereich der Richtlinie nicht niedergelassen ist.

Dies ist vorliegend nicht der Fall. Der für die streitgegenständliche Datenverarbeitung Verantwortliche besitzt im Sinne von Art. 4 Abs. 1 Richtlinie 95/46/EG im Gebiet der Europäischen Union eine Niederlassung.

(1) Bei natürlichem Verständnis des Begriffs der Niederlassung erscheint nicht zweifelhaft, dass der Geschäftsbetrieb der Antragstellerin in Dublin eine Niederlassung im Sinne von Art. 4 Abs. 1 Richtlinie 95/46/EG darstellt (vgl. auch Schleswig-Holsteinisches OVG, Beschl. v. 22.4.2013, 4 MB 11/13, juris, Rn. 13). Zwischen den Beteiligten ist unstrittig, dass die Antragstellerin in Irland über 900 Mitarbeiter beschäftigt und eine Abteilung unterhält, die auf Anfragen und Beschwerden reagiert. Zu den Maßnahmen, die sie ergreift, gehört es unter anderem, Inhalte oder Profile zu sperren, die gegen geltendes Recht oder Nutzungsbedingungen verstoßen. Die Antragstellerin unterhält nach ihren Angaben in Irland auch eine Rechtsabteilung, die dafür verantwortlich sei, dass das soziale Netzwerk im Einklang mit den anwendbaren datenschutzrechtlichen Bestimmungen des irischen und europäischen Rechts betrieben werde.

(2) Darüber hinaus wird es sich nach dem zugrunde zu legenden Sachverhalt bei dem Geschäftsbetrieb der Antragstellerin in Dublin auch um eine Niederlassung des im Sinne

von § 3 Abs. 7 BDSG, Art. 2 lit. d Richtlinie 95/46/EG für die Datenverarbeitung Verantwortlichen handeln. Auch die Beteiligten gehen hiervon übereinstimmend aus. Es wird jedoch offen bleiben können, ob die Antragstellerin alleine, gemeinsam mit der Muttergesellschaft F., Inc. oder gar die F., Inc. alleine für die streitige Datenverarbeitung verantwortlich ist (vgl. hierzu und zum Folgenden bereits Schleswig-Holsteinisches VG, Beschl. v. 14.2.2013, 8 B 61/12, juris, Rn. 26-31, sowie im Nachgang Schleswig-Holsteinisches OVG, Beschl. v. 22.4.2013, 4 MB 11/13, juris, Rn. 20). Denn aufgrund der entsprechenden konzernrechtlichen Verflechtungen dürfte der Geschäftsbetrieb der Antragstellerin in Irland nicht nur als Niederlassung der Antragstellerin, sondern auch als eine Niederlassung der F., Inc. zu qualifizieren sein.

cc) Die Anwendung deutscher datenschutzrechtlicher Bestimmungen folgt voraussichtlich auch nicht aus § 1 Abs. 5 Satz 1 BDSG in Verbindung mit Art. 4 Abs. 1 lit. a Richtlinie 95/46/EG. Denn nach Auffassung der Kammer ist, wenn aufgrund von Niederlassungen der verantwortlichen Stelle in mehreren Mitgliedsstaaten mehrere mitgliedstaatliche Datenschutzregime in Betracht kommen, das Recht desjenigen Mitgliedsstaats anzuwenden, in dem sich diejenige Niederlassung befindet, die zu der streitigen Datenverarbeitung den engsten Bezug hat [unten (1)]. Danach sind deutsche datenschutzrechtliche Bestimmungen, auf die die angefochtene Anordnung allein gestützt wird, auf die streitige Datenverarbeitung nicht anzuwenden [unten (2)].

(1) Gemäß § 1 Abs. 5 Satz 1 Halbsatz 1 BDSG können deutsche datenschutzrechtliche Bestimmungen grundsätzlich nicht angewendet werden, sofern eine in einem anderen Mitgliedsstaat der Europäischen Union belegene verantwortliche Stelle personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt. Gemäß § 1 Abs. 5 Satz 1 Halbsatz 2 BDSG sind jedoch ausnahmsweise deutsche datenschutzrechtliche Bestimmungen anzuwenden, sofern die Verarbeitung von Daten im Bundesgebiet durch eine im Bundesgebiet belegene Niederlassung erfolgt.

§ 1 Abs. 5 Satz 1 BDSG muss als Umsetzung von Art. 4 Abs. 1 lit. a Richtlinie 95/46/EG in dessen Sinne ausgelegt und angewandt werden. Nach Art. 4 Abs. 1 lit. a Richtlinie 95/46/EG wendet jeder Mitgliedsstaat die Vorschriften, die er zur Umsetzung der Richtlinie erlässt, auf alle Verarbeitungen personenbezogener Daten an, die im Rahmen der Tätigkeiten einer Niederlassung ausgeführt werden, die der für die Verarbeitung Verant-

wortliche im Hoheitsgebiet dieses Mitgliedsstaats besitzt. Gemäß Art. 4 Abs. 1 lit. a Satz 2 Richtlinie 95/46/EG hat der Verantwortliche, wenn er eine Niederlassung im Hoheitsgebiet mehrerer Mitgliedsstaaten besitzt, die notwendigen Maßnahmen zu ergreifen, damit jede dieser Niederlassungen die im jeweils anwendbaren einzelstaatlichen Recht festgelegten Verpflichtungen einhält. Nationale datenschutzrechtliche Bestimmungen sind demnach nicht anzuwenden, wenn die für die streitige Datenverarbeitung verantwortliche Stelle nur in einem anderen Mitgliedsstaat der Europäischen Union niedergelassen ist (vgl. EuGH, Schlussanträge vom 25.6.2015, C-230/14, juris, Rn. 42 – Weltimmo) oder die streitige Datenverarbeitung nicht „im Rahmen der Tätigkeiten“ der nationalen Niederlassung erfolgt.

Im vorliegenden Fall wird unter Berücksichtigung der Rechtsprechung des Europäischen Gerichtshofs zwar davon auszugehen sein, dass die für die Datenverarbeitung verantwortliche Stelle (auch) im Bundesgebiet niedergelassen ist [siehe unten (a)]. Nach Auffassung der Kammer findet die streitige Datenverarbeitung jedoch nicht im Sinne von Art. 4 Abs. 1 lit. a Satz 1 Richtlinie 95/46/EG „im Rahmen der Tätigkeiten“ dieser Niederlassung statt [siehe unten (b)].

(a) F. Germany wird im Sinne des Art. 4 Abs. 1 lit. a Richtlinie 95/46/EG als Niederlassung sowohl der F., Inc. als auch der Antragstellerin zu qualifizieren sein.

Der Begriff der Niederlassung ist nicht legal definiert. Er ist im Hinblick auf eine effektive Umsetzung der Richtlinie auszulegen. Der Unionsgesetzgeber äußert sich in Erwägungsgrund 19 der Richtlinie 95/46/EG zum Begriff der Niederlassung. Demnach setzt eine Niederlassung im Hoheitsgebiet eines Mitgliedsstaats (lediglich) die effektive und tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung voraus. Die Rechtsform einer solchen Niederlassung, die eine Agentur oder eine Zweigstelle sein könne, sei in dieser Hinsicht nicht maßgeblich. Im Sinne der Richtlinie kann demzufolge ein Unternehmen auch an einem anderen Ort als demjenigen seiner registerlichen Eintragung niedergelassen sein (vgl. EuGH, Schlussanträge vom 25.6.2015, C-230/14, juris, Rn. 28 – Weltimmo). Nach der Rechtsprechung des Europäischen Gerichtshofs sind an die Voraussetzung einer Niederlassung im Sinne der Richtlinie 95/46/EG nur geringe Anforderungen zu stellen. Demnach setzt die Richtlinie beispielsweise keine (eingetragene) gesellschaftsrechtliche Niederlassung voraus. Der Begriff der Niederlassung sei flexibel konzipiert und

nicht formalistisch zu bestimmen. Insbesondere bei Unternehmen, die Leistungen ausschließlich über das Internet anbieten, sei sowohl der Grad an Beständigkeit der Einrichtung als auch die effektive Ausübung der wirtschaftlichen Tätigkeiten im Mitgliedsstaat der fraglichen Niederlassung unter Beachtung des besonderen Charakters dieser Tätigkeiten und der in Rede stehenden Dienstleistungen maßgeblich (EuGH, Urt. v. 1.10.2015, C-230/14, Rn. 29 – Weltimmo). Das Vorhandensein eines einzigen Vertreters könne unter bestimmten Umständen ausreichen, um eine feste Einrichtung zu begründen, wenn dieser mit einem ausreichenden Grad an Beständigkeit mit den für die Erbringung der betreffenden konkreten Dienstleistungen erforderlichen Mitteln im fraglichen Mitgliedsstaat tätig sei. Dies folge aus dem Ziel der Richtlinie 95/46/EG, einen wirksamen und umfassenden Schutz des Rechts auf Privatleben zu gewährleisten und Umgehungen zu vermeiden (EuGH, Urt. v. 1.10.2015, C-230/14, Rn. 30 – Weltimmo).

Nach diesen Maßstäben dürfte F. Germany eine Niederlassung sowohl der F., Inc. als auch der Antragstellerin darstellen. Dem dürfte im Hinblick auf die Beziehungen zwischen F. Germany und der Antragstellerin nicht entgegenstehen, dass F. Germany konzernrechtlich lediglich als Schwester der Antragstellerin zu qualifizieren sein könnte. Denn nach dem unstreitigen Sachverhalt ist F. Germany als eingetragene Gesellschaft mit beschränkter Haftung mit über 50 Mitarbeitern an den Standorten Hamburg und Berlin tätig und unterstützt die Antragstellerin bei der geschäftsmäßigen Erbringung des Dienstes F.. Hierdurch dient F. Germany kraft konzernrechtlicher Verflechtungen innerhalb des F.-Konzerns gleichzeitig auch der F., Inc.

(b) Nach Auffassung der Kammer ist jedoch nicht davon auszugehen, dass die streitige Datenverarbeitung im Sinne von Art. 4 Abs. 1 lit. a Satz 1 Richtlinie 95/46/EG „im Rahmen der Tätigkeiten“ von F. Germany ausgeführt wird. Das Merkmal „im Rahmen der Tätigkeiten“ ist gemäß dem Zweck der Vorschrift auszulegen und anzuwenden [unten (aa)]. Danach ist gemäß der Rechtsprechung des Europäischen Gerichtshofs in Sachen Google und Google Spain der Anwendungsbereich weit zu fassen, wenn der für die Datenverarbeitung Verantwortliche seinen Sitz außerhalb der Europäischen Union hat [unten (bb)]. Diese weite Auslegung des Merkmals „im Rahmen der Tätigkeiten“ kann nach Auffassung der Kammer auf den vorliegenden Fall allerdings nicht übertragen werden [unten (cc)]. Denn wenn über das Merkmal „im Rahmen der Tätigkeiten“ einer Niederlassung lediglich die Konkurrenz verschiedener mitgliedsstaatlicher Rechtsordnungen aufzulösen

ist, weil der für die Verarbeitung Verantwortliche in mehreren Mitgliedsstaaten niedergelassen ist, ist eine weite Auslegung nicht gerechtfertigt. In solchen Fällen ist nach Auffassung der Kammer das Recht jenes Staates anzuwenden, in dem sich diejenige Niederlassung befindet, mit deren Tätigkeit die streitige Datenverarbeitung am engsten verbunden ist [unten (dd)]. Dies steht auch im Einklang mit der Rechtsprechung des Europäischen Gerichtshofs in Sachen Weltimmo [unten (ee)].

(aa) Art. 4 Abs. 1 lit. a Richtlinie 95/46/EG will zur Bestimmung des anwendbaren Rechts hauptsächlich an den Ort einer Niederlassung des für die Verarbeitung Verantwortlichen anknüpfen (vgl. Schleswig-Holsteinisches OVG, Beschl. v. 22.4.2013, 4 MB 11/13, juris, Rn. 20; Artikel-29-Datenschutzgruppe, Stellungnahme 8/2010 zum anwendbaren Recht, 16.12.2010, WP 179, S. 11 f.). Als Kollisionsrecht der Richtlinie 95/46/EG erfüllt Art. 4 Abs. 1 lit. a Richtlinie 95/46/EG dabei eine doppelte Funktion: Die Vorschrift ermöglicht es zunächst, bei Vorhandensein einer relevanten Niederlassung des für die Verarbeitung Verantwortlichen das Datenschutzrecht der Union vermittelt durch das gemäß der Richtlinie gestaltete Datenschutzrecht des Mitgliedsstaats der Niederlassung auch dann zur Anwendung zu bringen, wenn die „eigentliche“ Datenverarbeitung in einem Drittstaat erfolgt (vgl. EuGH, Schlussanträge vom 25.6.2015, C-230/14, Rn. 23 – Weltimmo). Darüber hinaus ist Art. 4 Abs. 1 lit. a Richtlinie 95/46/EG zu entnehmen, welches Recht im Verhältnis der Mitgliedsstaaten zueinander anzuwenden ist, wenn bei grenzüberschreitenden Sachverhalten mehrere mitgliedersstaatliche Rechtsordnungen infrage kommen. Die Vorschrift fungiert dann als Kollisionsnorm zwischen den Rechtsordnungen der verschiedenen Mitgliedsstaaten (vgl. EuGH, Schlussanträge vom 25.6.2015, C-230/14, Rn. 23 – Weltimmo; ferner Artikel-29-Datenschutzgruppe, Stellungnahme 8/2010 zum anwendbaren Recht, 16.12.2010, WP 179, S. 12).

Diese zweite Funktion von Art. 4 Abs. 1 lit. a Richtlinie 95/46/EG ist für den vorliegenden Fall entscheidend. Da sowohl der Geschäftsbetrieb der Antragstellerin in Dublin als auch der Betrieb von F. Germany im Bundesgebiet als Niederlassung des für die Datenverarbeitung Verantwortlichen im Sinne von Art. 4 Abs. 1 lit. a Richtlinie 95/46/EG zu qualifizieren sein dürften, ist die Konkurrenz irischer und deutscher datenschutzrechtlicher Bestimmungen über das Merkmal „im Rahmen der Tätigkeiten“ aufzulösen.

(bb) Zwar zwingt insbesondere die Entscheidung des Europäischen Gerichtshofs in Sachen Google und Google Spain (EuGH, Urt. v. 13.5.2014, C-131/12, juris) zur Prüfung, ob die streitige Datenverarbeitung trotz deren besonderen Aufgabenbereichs (auch) „im Rahmen der Tätigkeiten“ von F. Germany ausgeführt wird. Denn die Voraussetzung „im Rahmen der Tätigkeiten“ einer Niederlassung soll (ebenso wie der Begriff der Niederlassung) hiernach weit auszulegen sein (vgl. EuGH, Urt. v. 13.5.2014, C-131/12, juris, Rn. 53 – Google und Google Spain). Es sei nicht erforderlich, dass die angegriffene Verarbeitung personenbezogener Daten von der betreffenden Niederlassung selbst ausgeführt werde. Die Richtlinie verlange lediglich, dass die Datenverarbeitung „im Rahmen der Tätigkeiten“ der Niederlassung ausgeführt werde (EuGH, Urt. v. 13.5.2014, C-131/12, juris, Rn. 52 – Google und Google Spain). Für den Fall des Betriebs einer Internetsuchmaschine ergebe sich aus dem Schutzzweck der Richtlinie 95/46/EG, dass die Verarbeitung personenbezogener Daten, die für den Dienst der Suchmaschine erfolge, die von einem Unternehmen betrieben werde, das seinen Sitz in einem Drittstaat habe, jedoch in einem Mitgliedsstaat über eine Niederlassung verfüge, „im Rahmen der Tätigkeiten“ dieser Niederlassung ausgeführt würden, wenn diese Niederlassung die Aufgabe habe, in dem Mitgliedsstaat für die Förderung des Verkaufs der angebotenen Werbeflächen der Suchmaschine, mit denen die Dienstleistung der Suchmaschine rentabel gemacht werden solle, und für den Verkauf der Werbeflächen selbst zu sorgen. Unter solchen Umständen seien die Tätigkeiten des Suchmaschinenbetreibers und die seiner Niederlassung in dem betreffenden Mitgliedsstaat untrennbar miteinander verbunden, da die die Werbeflächen betreffenden Tätigkeiten das Mittel darstellten, um die in Rede stehende Suchmaschine wirtschaftlich rentabel zu machen, und die Suchmaschine gleichzeitig das Mittel sei, das die Durchführung dieser Tätigkeiten ermögliche (EuGH, Urt. v. 13.5.2014, C-131/12, juris, Rn. 55 f. – Google und Google Spain).

Demnach könnte mit dem Europäischen Gerichtshof davon auszugehen sein, dass im Sinne der Richtlinie eine Datenverarbeitung bereits dann „im Rahmen der Tätigkeiten“ einer Niederlassung erfolgt, wenn die Niederlassung mit ihrer Tätigkeit der wirtschaftlichen Rentabilität des Internetangebots im nationalen Markt dient und das Internetangebot gleichzeitig das Mittel ist, dass die Tätigkeit der Niederlassung ermöglicht. Übertragen auf den zu entscheidenden Fall könnte dies die Annahme nahe legen, dass die streitige Datenverarbeitung im Rahmen der Tätigkeit von F. Germany erfolgt. Denn die Tätigkeit von F. Germany im deutschen Markt trägt zur Rentabilität des Dienstes F. insgesamt bei, in-

dem F. Germany den F.-Konzern und vor allem die Antragstellerin zum Beispiel bei der Platzierung von Werbung von Gewerbetreibenden unterstützt. Diese Werbung wird deutschen Nutzern wie der Betroffenen über das Netzwerk zugänglich gemacht. Die Tätigkeit von F. Germany könnte insoweit als nicht trennbar von der streitigen Datenverarbeitung, der Verarbeitung und Anzeige der Profile von Nutzern unter deren Klarnamen, zu qualifizieren sein (das Kriterium der „wirtschaftlichen Untrennbarkeit“ nunmehr auch als hinreichend erachtend als Voraussetzung der Anwendung des Rechts des Mitgliedsstaats der Niederlassung: Artikel-29-Datenschutzgruppe, Update of Opinion 8/2010 on applicable law [...], 16.12.2015, WP 179 update, dort S. 4 ff.).

(cc) Dass die Tätigkeiten von F. Germany wirtschaftlich von der streitigen Datenverarbeitung nicht zu trennen sind, vermag nach Auffassung der Kammer nicht zu rechtfertigen, für von der Verarbeitung Betroffene im Bundesgebiet deutsche datenschutzrechtliche Bestimmungen anzuwenden (anders wohl Artikel-29-Datenschutzgruppe, Update of Opinion 8/2010 on applicable law [...], 16.12.2015, WP 179 update, dort insb. S. 7 und Annex 1, S. 2 f.).

Einer Übertragung der Rechtsprechung des Europäischen Gerichtshofs in Sachen Google und Google Spain steht hier bereits entgegen, dass jene Entscheidung nicht den Konflikt von Rechtsordnungen innerhalb der Union betraf, sondern dem Unionsrecht überhaupt zur Geltung verhelfen wollte. Der Europäische Gerichtshof hat deshalb ausgeführt, der Richtliniengeber habe einen besonders weiten räumlichen Anwendungsbereich der Richtlinie 95/46/EG vorgesehen, um zu vermeiden, dass der gemäß der Richtlinie gewährleistete Schutz einer Person vorenthalten und umgangen werde (EuGH, Urt. v. 13.5.2014, C-131/12, juris, Rn. 54 – Google und Google Spain, unter Verweis auf Erwägungsgründe 18-20 und Art. 4 Richtlinie 95/46/EG). Es könne nicht angehen, dass die Verarbeitung personenbezogener Daten, die zum Betrieb einer Suchmaschine ausgeführt werde, den in der Richtlinie 95/46/EG vorgesehenen Verpflichtungen und Garantien entzogen werde. Denn dies schränke die praktische Wirksamkeit der Richtlinie (effet utile) und den wirksamen und umfassenden Schutz der Grundrechte und Grundfreiheiten natürlicher Personen, die mit ihr gewährleistet werden sollten, ein (vgl. EuGH, Urt. v. 13.5.2014, C-131/12, juris, Rn. 58 – Google und Google Spain). Damit hatte der Europäische Gerichtshof aber einen Fall zu entscheiden, der sich wesentlich von dem vorliegenden unterscheidet. Im Fall „Google und Google Spain“ verfügte der für die streitige Datenverarbeitung Verant-

wortliche nach der Auslegung des Europäischen Gerichtshofs zwar über eine Niederlassung in dem Unionsstaat, dessen Datenschutzbehörden gegenüber dem Verantwortlichen tätig geworden sind. Die dort streitige Datenverarbeitung wurde jedoch von jemandem kontrolliert, der nicht im räumlichen Geltungsbereich der Richtlinie 95/46/EG saß. Es stand deshalb zu befürchten, die personenbezogenen Daten betroffener Unionsbürger würden entgegen den Standards der Richtlinie 95/46/EG verarbeitet. Insoweit sind die Fallkonstellationen aber nicht vergleichbar. Die im vorliegenden Fall für die Datenverarbeitung (mit-)verantwortliche Stelle besitzt eine Niederlassung in einem Mitgliedsstaat der Europäischen Union. Deshalb ist im vorliegenden Fall nicht zu befürchten, dass von der streitigen Datenverarbeitung betroffenen Unionsbürgern der Schutz der Richtlinie 95/46/EG versagt bleiben könnte. Aufgrund der Niederlassung des F.-Konzerns in Dublin kommt die Richtlinie 95/46/EG vermittelt durch das Recht Irlands jedenfalls zur Geltung. Dass in einer solchen Konstellation das relativ hohe Niveau des Schutzes Betroffener durch die Richtlinie 95/46/EG gewährleistet wäre, räumt auch die Artikel-29-Datenschutzgruppe in ihrer aktualisierten Veröffentlichung ein (vgl. Artikel-29-Datenschutzgruppe, Update of Opinion 8/2010 on applicable law [...], WP 179 update, S. 6).

(dd) Im Fall einer solchen Konkurrenz des Datenschutzrechts verschiedener Mitgliedsstaaten ist nach vorläufiger Auffassung der Kammer das Recht jenes Staates anzuwenden, in dem sich diejenige Niederlassung befindet, mit deren Tätigkeit die streitige Datenverarbeitung am engsten verbunden ist.

In Bezug auf den hier zu lösenden Konflikt unterschiedlicher nationaler Datenschutzbestimmungen der Mitgliedstaaten hat bereits die Artikel-29-Datenschutzgruppe in ihrer Stellungnahme aus dem Jahr 2010 zu Recht darauf hingewiesen, dass das Kollisionsrecht der Richtlinie 95/46/EG nicht nur Schutzlücken verhindern, sondern bei Niederlassungen der verantwortlichen Stelle in mehreren Mitgliedsstaaten auch Überschneidungen einzelstaatlicher Rechtsordnungen vermeiden will. Die Anwendung des Kriteriums „im Rahmen der Tätigkeiten“ der Niederlassung werde dann besonders relevant. Es solle verhindert werden, dass mehrere einzelstaatliche Rechtsordnungen auf dieselbe Datenverarbeitung Anwendung finden (vgl. Artikel-29-Datenschutzgruppe, Stellungnahme 8/2010 zum anwendbaren Recht, WP 179, S. 12; soweit ersichtlich durch Update nicht aufgegeben). Unterschiedliche rechtliche Maßstäbe für identische Datenverarbeitungsvorgänge dürften nach Art. 4 Abs. 1 lit. a Satz 2 Richtlinie 95/46/EG nur dann hinzunehmen sein, wenn da-

tenverarbeitende Niederlassungen in mehreren Mitgliedstaaten angesiedelt sind und dort – für ihren jeweiligen räumlichen Bereich – inhaltlich identische Aufgaben wahrnehmen. Dann dürfte die Beachtung des jeweiligen nationalen Datenschutzrechts einer unionsweiten Rechtseinheitlichkeit vorgehen.

Wenn Niederlassungen in mehreren Mitgliedsstaaten existieren, dürfte demnach das anzuwendende mitgliedsstaatliche Recht nach der Tätigkeit zu bestimmen sein, die die jeweilige Niederlassung ausübt (vgl. Artikel-29-Datenschutzgruppe, Stellungnahme 8/2010 zum anwendbaren Recht, 16.12.2010, WP 179, S. 12). Wird die Datenverarbeitung „im Rahmen der Tätigkeiten“ von Niederlassungen in mehreren Mitgliedsstaaten ausgeführt, wird genau auf die Tätigkeiten abzustellen sein, in deren Rahmen die Verarbeitung stattgefunden hat (vgl. auch EuGH, Schlussanträge vom 25.6.2015, C-230/14, juris, Rn. 40 – Weltimmo). Maßgeblich ist der Ort derjenigen Niederlassung, die im Mittelpunkt der datenverarbeitenden Tätigkeit steht (vgl. Schreibauer, in: Auernhammer, BDSG, 4. Aufl. 2014, Vorbemerkung zu § 11 TMG, Rn. 25, zu § 1 Abs. 5 Satz 1 BDSG). Dabei wird zu berücksichtigen sein, in welchem Maß sich die fraglichen Niederlassungen an der Datenverarbeitung beteiligen. Um feststellen zu können, ob die einzelne Niederlassung als Anknüpfungspunkt für die Anwendung ihres nationalen Datenschutzrechts geeignet ist, sind die Tätigkeiten der einzelnen Niederlassung gegeneinander abzugrenzen. Stellt sich dabei heraus, dass eine Niederlassung personenbezogene Daten nicht vorrangig im Rahmen ihrer eigenen Tätigkeiten, sondern im Rahmen der Tätigkeiten einer anderen Niederlassung verarbeitet, sind die datenschutzrechtlichen Bestimmungen des Mitgliedsstaats anzuwenden, in dem sich die andere Niederlassung befindet (vgl. Artikel-29-Datenschutzgruppe, Stellungnahme 8/2010 zum anwendbaren Recht, 16.12.2010, WP 179, S. 17 f.; modifiziert und teilweise aufgegeben durch Update of Opinion 8/2010 on applicable law [...], 16.12.2015, WP 179 update, vgl. dort z.B. Annex 1, S. 3).

Für diese Auslegung und Anwendung des Merkmals „im Rahmen der Tätigkeiten“ der Niederlassung spricht vor allem, dass hierdurch vermieden werden kann, dass beispielsweise die Anbieter grenzüberschreitender Telemedien im Hinblick auf ein- und dieselbe Datenverarbeitung eine Vielzahl unterschiedlicher mitgliedsstaatlicher datenschutzrechtlicher Bestimmungen beachten müssten (vgl. Artikel-29-Datenschutzgruppe, Stellungnahme 8/2010 zum anwendbaren Recht, 16.12.2010, WP 179, S. 12; offenbar durch Update nicht infrage gestellt). Ein solcher Art erleichterter grenzüberschreitender Verkehr perso-

nenbezogener Daten dürfte zunächst im Einklang stehen mit dem übergeordneten Zweck eines möglichst freien europäischen Binnenmarktes. Dies motivierte auch den Richtliniengeber im Bereich des Datenschutzes. Die Richtlinie 95/46/EG bezweckt ausdrücklich ein gleichwertiges Schutzniveau hinsichtlich des Rechts der Verarbeitung personenbezogener Daten in den Mitgliedsstaaten, um den innergemeinschaftlichen Verkehr personenbezogener Daten zu erleichtern (vgl. insbesondere Erwägungsgründe 7-9 Richtlinie 95/46/EG). Anhaltspunkte für die Bedeutung dieses Aspekts dürften auch die Regelungen des Richtliniengebers im Bereich der „Dienste der Informationsgesellschaft“ liefern. Auch wenn die Richtlinie 2000/31/EG gemäß Art. 1 Abs. 5 lit. b Richtlinie 2000/31/EG ausdrücklich keine Geltung für Fragen des Datenschutzes im Zusammenhang mit „Diensten der Informationsgesellschaft“ beansprucht (vgl. hierzu bereits oben), dürfte die Vermeidung von Überschneidungen einzelstaatlichen Datenschutzrechts auch im Interesse eines möglichst freien Binnenmarktes für Telemedien liegen. Für den Bereich der „Dienste der Informationsgesellschaft“ wünscht sich der Richtliniengeber ausdrücklich, dass die Dienste der Informationsgesellschaft grundsätzlich dem Rechtssystem desjenigen Mitgliedsstaates unterworfen werden, in dem deren Anbieter niedergelassen ist, um den freien Dienstleistungsverkehr und die Rechtssicherheit für Anbieter und Nutzer wirksam zu gewährleisten (vgl. Erwägungsgrund 22 Richtlinie 2000/31/EG). Solche Zwecke billigte offenbar auch der deutsche Gesetzgeber bei der Umsetzung der Richtlinie 95/46/EG in § 1 Abs. 5 Satz 1 BDSG. Ausweislich der Gesetzesbegründung zum BDSG bezweckt Art. 4 Abs. 1 lit. a Richtlinie 95/46/EG unter anderem, dass Unternehmen ihr gewohntes nationales Datenschutzrecht „exportieren“ dürften und sich nicht durch unbekannte Datenschutzvorschriften in ihrer unternehmerischen Tätigkeit eingeschränkt sehen müssten. Die Regelung einer Ausnahme für Datenverarbeitungen durch Niederlassungen im Bundesgebiet diene der Rechtssicherheit insbesondere im Zusammenhang mit den Schutzrechten der von derartigen Datenverarbeitungen Betroffenen (vgl. BR-Drucks. 461/00, S. 76).

Demgegenüber will die Artikel-29-Datenschutzgruppe nunmehr offenbar unter bestimmten Voraussetzungen in Kauf nehmen, ein- und dieselbe Datenverarbeitung einer verantwortlichen Stelle im Falle von Niederlassungen in mehreren Mitgliedsstaaten den jeweiligen datenschutzrechtlichen Bestimmungen dieser Mitgliedsstaaten zu unterwerfen. Ausgehend von der Entscheidung des Europäischen Gerichtshofs in Sachen Google und Google Spain soll dies der Fall sein, wenn eine untrennbare wirtschaftliche Verbindung zwischen der fraglichen Datenverarbeitung und der Tätigkeit der mitgliedstaatlichen Nie-

derlassung wie im Falle von Google und Google Spain bestehe. Hintergrund dieser Auffassung ist es offenbar, datenverarbeitenden Unternehmen im Hinblick auf die unterschiedlichen mitgliedstaatlichen Standards in der Umsetzung der Richtlinie 95/46/EG einen „one-stop-shop“ des niedrigsten mitgliedstaatlichen Datenschutzniveaus zu versagen (vgl. Artikel-29-Datenschutzgruppe, Update of Opinion 8/2010 on applicable law [...], 16.12.2015, WP 179 update, S. 6).

Hierbei dürfte es sich jedoch um ein rechtspolitisches Ziel handeln, das noch nicht aus dem geltenden Recht hergeleitet werden kann. Aktuell unterschiedliche Datenschutzniveaus der Mitgliedstaaten dürfen derzeit nicht durch eine übermäßige, den Wortlaut der Richtlinie strapazierende Ausdehnung des Anwendungsbereichs von Art. 4 Abs. 1 lit. a Richtlinie 95/46/EG ausgeglichen werden, da es hierfür auf der Grundlage heutigen Unionsrechts keinen Anlass gibt. Insbesondere muss insoweit keinem unionsrechtlichen Anliegen zur praktischen Wirksamkeit verholfen werden.

Die im vorliegenden Fall streitige Datenverarbeitung deutschen datenschutzrechtlichen Bestimmungen nicht zu unterwerfen, erscheint als mit dem Zweck der Richtlinie 95/46/EG durchaus vereinbar, den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten zu gewährleisten (vgl. etwa Art. 1 Abs. 1 Richtlinie 95/46/EG). Nach Auffassung der Kammer vermag dieser Zweck eine über den Wortlaut hinausreichende Auslegung und Anwendung von Art. 4 Abs. 1 lit. a Richtlinie 95/46/EG nicht zu rechtfertigen, wenn die Vorschrift als innergemeinschaftliche Kollisionsnorm heranzuziehen ist. Bei der Bestimmung des anzuwendenden mitgliedstaatlichen Datenschutzrechts kann ein besonders weiter Anwendungsbereich etwa der Voraussetzung „im Rahmen der Tätigkeiten“ einer Niederlassung insbesondere nicht damit gerechtfertigt werden, der betroffene Unionsbürger werde ansonsten nicht in den Genuss des durch die Richtlinie gewährleisteten Datenschutzniveaus kommen. Denn die grundsätzliche Gewährleistung des Schutzes, den die Richtlinie 95/46/EG Betroffenen bieten will, steht in einem solchen Fall, vermittelt durch die der Umsetzung der Richtlinie dienenden datenschutzrechtlichen Bestimmungen der beteiligten Mitgliedstaaten, nicht infrage (vgl. auch Artikel-29-Datenschutzgruppe, Update of Opinion 8/2010 on applicable law [...], 16.12.2015, WP 179 update, S. 6).

Indem der europäische Gesetzgeber 1995 für den Bereich des Datenschutzes das Instrument der Richtlinie wählte, nahm er unterschiedliche Standards der Umsetzung in den Mitgliedsstaaten in Kauf und etablierte unionsweit lediglich einen Mindestschutz. Aufgrund der Möglichkeit datenverarbeitender Unternehmen aus Drittstaaten, den Ort ihrer Niederlassung in der Union frei wählen zu können, hat ein solch unterschiedliches Schutzniveau bei gleichzeitiger Verfolgung des Ziels, dieselbe Datenverarbeitung in der Union möglichst nur einem nationalen Schutzregime zu unterwerfen, zwangsläufig zur Folge, dass grenzüberschreitende Datenverarbeitung dem Datenschutzregime eines anderen Mitgliedstaates unterfallen kann. Hätte der europäische Gesetzgeber bereits bisher ein in allen Mitgliedsstaaten gleiches Datenschutzrecht gewährleisten wollen, hätte er sich des Instruments der Verordnung bedienen können, wie nunmehr mit der Datenschutz-Grundverordnung geplant. Diese basiert gerade auf der Erkenntnis, dass die Richtlinie 95/46/EG erhebliche Unterschiede im Datenschutzniveau der einzelnen Mitgliedstaaten nicht verhindern konnte (vgl. Vorerwägung Nr. 7 des Entwurfs der Datenschutz-Grundverordnung in der Fassung vom 28.1.2016), und nimmt dies zum Anlass, künftig einen gleichmäßigen, unionsweit wirksamen Datenschutz zu etablieren, unabhängig vom Sitz der Niederlassung eines für Datenverarbeitung Verantwortlichen (Vorerwägung Nr. 19 des Entwurfs der Datenschutz-Grundverordnung in der Fassung vom 28.1.2016). Erst die Datenschutz-Grundverordnung wird deshalb gegebenenfalls gewährleisten können, dass zugleich beide angestrebten Ziele – ein hohes Datenschutzniveau und unionsweite Einheitlichkeit des Rechts – erreicht werden können.

Bislang jedoch ist es noch mit dem Willen des Richtliniengebers vereinbar, dass Mitgliedsstaaten zu Gunsten der Rechtseinheitlichkeit in der Union unter Umständen auf ihr besonders hohes oder spezifisches nationales Datenschutzniveau verzichten müssen. So hält es der Richtliniengeber gemäß Erwägungsgrund 18 Satz 1 Richtlinie 95/46/EG für notwendig, aber ausdrücklich auch für ausreichend, dass auf eine in der Gemeinschaft erfolgte Verarbeitung personenbezogener Daten die Rechtsvorschriften nur eines Mitgliedsstaats angewandt werden. Um zu vermeiden, dass einer Person der gemäß der Richtlinie gewährleistete Schutz vorenthalten werde, müssten auf jede in der Gemeinschaft erfolgte Verarbeitung personenbezogener Daten die Rechtsvorschriften eines Mitgliedsstaats angewandt werden. Darüber hinausgehend soll (nur) auf diejenigen Datenverarbeitungen, die von einem Dritten für den in einem anderen Mitgliedsstaat niederge-

lassenen Verantwortlichen vorgenommen werden, die Rechtsvorschriften des Staates des Dritten angewandt werden (vgl. Erwägungsgrund 18 Satz 2 Richtlinie 95/46/EG).

(ee) Eine Auslegung und Anwendung der Voraussetzung „im Rahmen der Tätigkeiten“ der Niederlassung, die zu einer Anwendung deutscher datenschutzrechtlicher Bestimmungen auf die streitige Datenverarbeitung führte, folgt nach Auffassung der Kammer schließlich auch nicht aus der Rechtsprechung des Europäischen Gerichtshofs im zuletzt entschiedenen Fall Weltimmo. Im dortigen Verfahren befasste sich der Gerichtshof vor allem mit der Frage, ob die für die dort streitige Datenverarbeitung verantwortliche Stelle im Sinne der Richtlinie 95/46/EG trotz ihrer Eintragung in ein slowakisches Register in Ungarn im datenschutzrechtlich relevanter Weise niedergelassen war (vgl. EuGH, Urt. v. 1.10.2015, C-230/14, juris, Rn. 25-34 – Weltimmo). Dort war nur der Ort der Niederlassung streitig, nicht jedoch, ob die Datenverarbeitung auch im Rahmen deren Tätigkeit erfolgte (vgl. EuGH, Schlussanträge vom 25.6.2015, C-230/14, juris, Rn. 26 – Weltimmo). Nachdem der Gerichtshof begründet hatte, dass das fragliche Unternehmen effektiv nur in Ungarn im Sinne der Richtlinie niedergelassen war, stand dann auch für ihn außer Zweifel, dass der Internetauftritt des Unternehmens, also die dort fragliche Datenverarbeitung, im Sinne von Art. 4 Abs. 1 lit. a Richtlinie 95/46/EG auch im Rahmen der Tätigkeit seiner ungarischen Niederlassung erfolgte (vgl. EuGH, Urt. v. 1.10.2015, C-230/14, juris, Rn. 38 – Weltimmo). Die Antragstellerin dürfte zu Recht darauf hinweisen, dass es der Gerichtshof (anders noch Generalanwalt Cruz Villalón, vgl. EuGH, Schlussanträge vom 25.6.2015, C-230/14, juris, Rn. 40 – Weltimmo) vermieden hat, die Fallgestaltung von Niederlassungen des Verantwortlichen in mehreren Mitgliedsstaaten zu entscheiden. Dessen ungeachtet dürfte die Entscheidung des Gerichtshofs vor dem Hintergrund ergangen sein, dass ein datenschutzrechtliches Vorgehen der slowakischen Behörden gegen das Unternehmen keinen Erfolg versprach. Offenbar war davon auszugehen, dass Weltimmo seinen Sitz mehrfach von einem Staat in den anderen verlegt hatte und an seinem registermäßigen Sitz in der Slowakei gar keine Tätigkeit ausübte (vgl. EuGH, Urt. v. 1.10.2015, C-230/14, Rn. 16 – Weltimmo; EuGH, Schlussanträge vom 25.6.2015, C-230/14, juris, Rn. 27 – Weltimmo). Die Gefahr, dass sich die Antragstellerin auf solche Weise einer effektiven Kontrolle durch die irischen Datenschutzbehörden entzöge, ist nicht behauptet oder ersichtlich.

(2) Nach vorstehenden Maßstäben sind auf die streitige Datenverarbeitung deutsche datenschutzrechtliche Bestimmungen nicht anzuwenden, da die streitige Datenverarbeitung nach dem der Entscheidung zugrunde zu legenden Sachverhalt mit der Tätigkeit der Niederlassung F.s bzw. der Antragstellerin in Dublin am engsten verbunden ist. Dies ist vor allem aufgrund des vorgelegten Data Transfer and Processing Agreement und des übrigen unstreitigen Vorbringens der Antragstellerin zu ihrer geschäftlichen Tätigkeit in Dublin und der geschäftlichen Tätigkeit von F. Germany anzunehmen. Nicht F. Germany, sondern die Antragstellerin ist gemäß den Nutzungsbedingungen Vertragspartnerin der Betroffenen. Die Antragstellerin verwaltet auch die Nutzerkonten, greift auf sie zu und sperrt sie in Fällen wie dem vorliegenden, wenn Zweifel an der Identität des Inhabers des Nutzerkontos aufkommen. Demgegenüber ist die Tätigkeit von F. Germany lediglich mittelbar, vor allem wirtschaftlich, mit der streitigen Datenverarbeitung verbunden.

III.

Die Entscheidung über die Kosten des Verfahrens beruht auf § 154 Abs. 1 VwGO. Die Festsetzung des Streitwertes folgt aus § 53 Abs. 2 in Verbindung mit § 52 Abs. 2 GKG.