

Abschrift

SCHLESWIG-HOLSTEINISCHES OBERVERWALTUNGSGERICHT



Az.: 4 LB 20/13
8 A 14/12

verkündet am 4. September 2014

Justizangestellte
als Urkundsbeamtin der Geschäftsstelle

IM NAMEN DES VOLKES URTEIL

In der Verwaltungsrechtssache

der Wirtschaftsakademie Schleswig-Holstein GmbH vertreten durch den Geschäftsführer,
Hans-Detlev-Prien-Straße 10, 24106 Kiel

Klägerin und Berufungsbeklagte,

Proz.-Bev.: [REDACTED]
[REDACTED]

g e g e n

das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD), vertreten
durch den Schleswig-Holsteinischen Datenschutzbeauftragten, Dr. Thilo Weichert,
Holstenstraße 98, 24103 Kiel,

Beklagter und Berufungskläger,

Beigeladen:

Facebook Ireland Limited, vertreten durch den Vorstand Sonia Flynn, Theodore Ulliyot,
Hanover Reach 5 - 7, 5-7 Hanover Quay 2 Dublin, Ireland

Proz.-Bev.: [REDACTED]
[REDACTED]

Streitgegenstand: Datenschutzrecht

hat der 4. Senat des Schleswig-Holsteinischen Oberverwaltungsgerichts auf die mündliche Verhandlung vom 4. September 2014 durch den Vorsitzenden Richter am Oberverwaltungsgericht [REDACTED], den Richter am Oberverwaltungsgericht [REDACTED], die Richterin am Oberverwaltungsgericht [REDACTED] sowie die ehrenamtlichen Richter [REDACTED] und [REDACTED] für Recht erkannt:

Die Berufung des Beklagten gegen das Urteil des Schleswig-Holsteinischen Verwaltungsgerichts - 8. Kammer - vom 9. Oktober 2013 wird zurückgewiesen.

Der Beklagte trägt die Kosten des Verfahrens.

Die außergerichtlichen Kosten der Beigeladenen sind erstattungsfähig.

Das Urteil ist hinsichtlich der Kosten vorläufig vollstreckbar.

Dem Beklagten wird nachgelassen, die Vollstreckung durch Sicherheitsleistungen in Höhe des zu vollstreckenden Betrages abzuwenden, wenn nicht der jeweilige Vollstreckungsgläubiger zuvor Sicherheit in Höhe des zu vollstreckenden Betrages leistet.

Die Revision wird zugelassen.

Tatbestand:

Die Klägerin wendet sich gegen eine datenschutzrechtliche Anordnung des Beklagten, nach der sie ihre Facebook-Seite (Fanpage) zu deaktivieren hat.

Die Klägerin ist ein in Form einer gemeinnützigen Gesellschaft mit beschränkter Haftung betriebenes Bildungsunternehmen, das unter anderem den Weiterbildungsauftrag der drei Industrie- und Handelskammern in Schleswig-Holstein wahrnimmt. In diesem Zusammenhang unterhält sie eine sogenannte Fanpage bei der Beigeladenen.

Fanpages sind spezielle Benutzeraccounts, die bei Facebook von Unternehmen, gemeinnützigen Einrichtungen, Künstlern und Prominenten eingerichtet werden können. Der Betreffende muss sich hierzu bei Facebook registrieren und kann dann die von Facebook unterhaltene Plattform dazu benutzen, sich den Nutzern dieser Plattform zu präsentieren und Äußerungen aller Art in den Medien- und Meinungsmarkt einzubringen. Nutzer der Plattform können eigene Beiträge auf der Plattform posten.

Betreiber von Fanpages bei Facebook können mit Hilfe des von Facebook kostenfrei zur Verfügung gestellten Werkzeuges „Facebook-Insights“ anonymisierte Statistik-Informationen über Nutzer erhalten. Die durch Facebook erstellten Statistiken enthalten Angaben über die Nutzung der Fanpage. Dazu gehören Informationen über den Nutzerzuwachs, die Demographie der Nutzer und über die Nutzung der einzelnen Funktionalitäten der Fanpage (vom Beklagten Reichweitenanalyse genannt).

Nach Anhörung der Klägerin ordnete der Beklagte mit Bescheid vom 3. November 2011 gemäß § 38 Abs. 5 S. 1 BDSG gegenüber der Klägerin an, dafür Sorge zu tragen, dass die von ihr bei Facebook betriebene Fanpage deaktiviert werde. Falls die Klägerin dieser Verpflichtung nicht innerhalb von 6 Wochen nach Zustellung des Bescheides nachkomme, werde gegen sie ein Zwangsgeld in Höhe von 5.000,00 € verhängt. Zur Begründung verwies der Beklagte darauf, dass Nutzungsdaten nach § 15 TMG (u.a. IP-Adresse, die Cookie-ID aus dem Cookie „datr“, Familien- und Vorname, Geburtsname) von Nutzern, welche die Fanpage der Klägerin aufriefen, nach § 15 Abs. 3 Satz 1 TMG für Zwecke der Werbung von Facebook erhoben würden, ohne dass die Klägerin als die nach § 12 Abs. 2 TMG i.V.m. § 3 Abs. 7 BDSG für die Datenverarbeitung datenschutzrechtlich verantwortliche Stelle den Nutzer über eine Widerspruchsmöglichkeit unterrichte. Die von Facebook zur Verfügung gestellte Infrastruktur erlaube es der Klägerin schon technisch nicht, einen Widerspruchmechanismus einzurichten. Selbst bei etwaigen Widersprüchen von Fanpagebesuchern gegen die Erstellung von Nutzungsprofilen bestehe für die Klägerin keine Möglichkeit, eine solche Datenverarbeitung durch Facebook für die Zukunft auszuschließen. Die angeordnete Maßnahme sei deshalb erforderlich. Des Weiteren verarbeite Facebook gewonnene Nutzungsdaten zu pseudonymen Nutzerprofilen, so dass in diesem Zusammenhang ein Verstoß gegen § 15 Abs. 3 S. 3 TMG vorliege, da Nutzungsprofile nicht mit Daten über die Träger des Pseudonyms zusammengefasst werden dürften.

Den von der Klägerin eingelegten Widerspruch begründete diese im Wesentlichen mit ihrer fehlenden Diensteanbiereigenschaft im Sinne des Telemediengesetzes sowie ihrer fehlenden datenschutzrechtlichen Verantwortung.

Mit Widerspruchsbescheid vom 16. Dezember 2011, zugegangen am 20. Dezember 2011, hat der Beklagte den Widerspruch zurückgewiesen.

Die Klägerin hat am 19. Januar 2012 Klage erhoben.

Sie hat geltend gemacht, dass es bereits an der Verarbeitung personenbezogener Daten fehle. Soweit im Rahmen der Registrierung bei Facebook von den Nutzern personenbezogene Daten wie Familien- und Vorname, Geburtsdatum etc. erhoben würden, beziehe sich dies allein auf das Nutzungsverhältnis zwischen dem Nutzer und Facebook. Inwiefern darüber hinaus seitens Facebook im Rahmen des Registrierungsvorgangs die IP-Adresse des Nutzers erhoben würde, sei ihr nicht bekannt. Gleiches gelte für das etwaige Setzen von Cookies. Die Erhebung von IP-Adressen und der Einsatz von Cookies seien auch nicht datenschutzrechtlich relevant, da es sich dabei nicht um personenbezogene Daten handele. Sie sei auch keine Diensteanbieterin. Sie nutze die Facebook-Plattform und die zur Verfügung gestellte Infrastruktur, um eigene Informationen zu verbreiten. Deshalb könne sie grundsätzlich Diensteanbieterin im Sinne des Telemediengesetzes sein, dies jedoch nur bezogen auf das eigene inhaltliche Angebot. Im Zusammenhang mit diesem Angebot erfolge von ihrer Seite aus auch keine Datenerhebung und auch keine Datenverwendung im Sinne von § 15 Abs. 1 TMG. Auch erstelle sie keinerlei Nutzungsprofile. Die Handlungen von Facebook könnten ihr nicht zugerechnet werden. Eine Auftragsdatenverarbeitung im Sinne von § 11 BDSG liege nicht vor. Insoweit würde die Auftragsdatenverarbeitung als verlängerter Arm, der für die Datenverarbeitung verantwortlichen Stelle, die stets Herrin der Daten bleibe, bezeichnet. Der Diensteanbieter bleibe bei der Datenverarbeitung verantwortliche Stelle, um seine datenschutzrechtliche Verantwortlichkeit nicht zu verlagern. Im Rahmen der Nutzung der Facebook-Infrastruktur bestünde diese Gefahr einer Auslagerung der Verantwortlichkeit hingegen schon im Ansatz nicht, da die Daten stets unmittelbar von Facebook und ohne ihre Mitwirkung verarbeitet würden. Facebook werde gerade nicht von ihr beauftragt, sondern stelle ihr die Dienste ungefragt zur Verfügung. Die Initiative gehe von Facebook aus. Vollständig anonymisierte statistische Berichte würden ihr lediglich als Nebenprodukt zur Verfügung gestellt.

Weiterhin finde auch keine Übermittlung personenbezogener Daten durch sie an Facebook statt. Eine Datenerhebung erfolge ausschließlich unmittelbar durch Facebook, ohne ihr Zutun. Sie habe weder Einfluss auf die technische Organisation der Facebook-Infrastruktur noch Sorge sie für die Ermittlung oder Generierung irgendwelcher Daten an Facebook. Eine eigenständige datenschutzrechtliche Verantwortlichkeit scheide deshalb bereits aus. Eine gemeinsame Entscheidung über die Erhebungs- und Verarbeitungszwecke der Daten durch eine Einigung zwischen Facebook und ihr bestehe nicht. Sie treffe keinerlei inhaltliche Entscheidung über Art, Umfang oder Zweck der Datenverarbeitung. Eine solche würde auch nicht dadurch begründet, dass Facebook ungefragt eine anonyme Nutzungsstatistik liefere. Schließlich habe der Beklagte das ihm nach § 38 Abs. 5 S. 1 BDSG eingeräumte Ermessen nicht bzw. nicht ordnungsgemäß ausgeübt.

Die Klägerin hat beantragt,

die getroffene Anordnung des Beklagten nach § 38 Abs. 5 S. 1 BDSG vom 3. November 2011 sowie den Widerspruchsbescheid des Beklagten vom 16. Dezember 2011 aufzuheben.

Der Beklagte hat beantragt,

die Klage abzuweisen.

Er hat die Auffassung vertreten, dass die Anordnung formell und materiell rechtmäßig sei. Die Anordnung der Deaktivierung sei eine Maßnahme im Sinne des § 38 Abs. 5 Satz 1 BDSG. Eine unternehmensinterne, rein administrative Nutzung durch Einzelpersonen und Pflege der Fanpage wäre weiterhin möglich. Für den Fall, dass Facebook für die Zukunft die festgestellten datenschutzrechtlichen Verstöße beseitige, wäre die deaktivierte Fanpage wieder zulässigerweise aktivierbar. Die auf der Facebook-Fanpage von der Klägerin eingestellten Inhalte könne diese nach einer Deaktivierung der Fanpage weiter nutzen. So wäre es etwa denkbar, dass sie die Inhalte nach der Deaktivierung im Rahmen anderer Dienste verwende.

Bei den verarbeiteten IP-Adressen und den Cookies handele es sich um personenbezogene Daten im Sinne von § 3 Abs. 1 BDSG. Durch die Beigeladene ebenso wie durch die Facebook Inc. (USA) fänden Datenschutzrechtsverstöße gegen §§ 13 Abs. 1, 15 Abs. 3

S. 1 und 2 TMG statt, für die die Klägerin als Diensteanbieterin nach § 12 Abs. 3 TMG iVm § 3 Abs. 7 BDSG (mit-)verantwortlich sei. Die Art. 29 - Datenschutzgruppe habe in einer Stellungnahme deutlich gemacht, dass Betreiber von Werbenetzwerken und Anbieter von Online-Inhalten gemeinsam als für die Datenverarbeitung verantwortliche Stelle anzusehen seien. Durch Konfigurierung der eigenen Webseite lösten Anbieter von Online-Inhalten letztlich auch die Übermittlung der IP-Adresse aus und stellten den ersten erforderlichen Schritt zur Ermöglichung der folgenden Verarbeitung der Daten für Werbezwecke dar. Vergleichbar erfolge auch die Datenverarbeitung durch die Klägerin und Facebook. Der Nutzer besuche die Fanpage der Klägerin, werde aber nicht deutlich darüber informiert, dass und vor allem welche seiner Nutzungs- wie auch seiner Registrierungsdaten, die er beim Anmeldevorgang bei Facebook eingegeben habe, für Werbezwecke verarbeitet würden. Mit dem Anlegen der Fanpage unternehme die Klägerin den entscheidenden Schritt dafür, dass unter anderem die IP-Adresse des Nutzers an Facebook geleitet werde, und löse beim Besuch des Nutzers auf der Fanpage diesen Übermittlungsvorgang aus, in dessen Folge Facebook beim Nutzer ein Cookie-ID setzen könne. Der Nutzer habe hiervon keine Kenntnis.

Die Klägerin leiste mit dem Anlegen der Fanpage einen willentlichen und adäquat kausalen Beitrag zu der Herbeiführung der rechtswidrigen Beeinträchtigungen der Nutzer. Die Klägerin könne sich ihrer Verantwortlichkeit nicht dadurch entziehen, dass sie den Störungszustand allein auf ein Verhalten von Facebook zurückführe. So habe das Landgericht Berlin entschieden, dass ein Nutzer, welcher E-Mail-Adressen von anderen Personen auf dem Facebook-Portal „hochlade“, den entscheidenden Beitrag dafür leiste, dass Facebook im Anschluss diese E-Mail-Adressen für Werbezwecke nutze, ohne dass hierfür eine Einwilligung der anderen Person vorliege. In diesem Zusammenhang seien Facebook und der jeweilige Nutzer als Mittäter im Sinne des § 830 Abs. 1 S. 1 BGB zu qualifizieren. Dies sei auf den vorliegenden Fall übertragbar. Selbst wenn der Klägerin die bevorstehenden Verletzungen datenschutzrechtlicher Vorschriften nicht bewusst gewesen sein sollten, so habe sie spätestens durch Veröffentlichungen und die Hinweise im Vorverfahren Kenntnis von dem mitverursachten Störungszustand erhalten. Die Aufrechterhaltung dieses Zustandes habe sie billigend in Kauf genommen. Einer Verantwortlichkeit könne die Klägerin sich auch nicht mit dem Verweis auf eine vermeintliche Einwilligung der Nutzer in die Datenverarbeitung durch Facebook entziehen.

Das Verwaltungsgericht hat durch Beschluss vom 21. November 2012, ergänzt durch Beschluss vom 25. März 2013, Facebook Ireland Ltd. mit Sitz in Dublin beigeladen.

Die Beigeladene hat beantragt,

den Bescheid vom 3. November 2011 in der Form des Widerspruchsbescheids vom 16. Dezember 2011 aufzuheben.

Die Beigeladene hat die Auffassung der Klägerin geteilt. Der Bescheid vom 3. November 2011 in der Fassung des Widerspruchsbescheides vom 16. Dezember 2011 sei bereits deshalb rechtswidrig, weil er durch die in der Anordnung ausdrücklich genannte Ermächtigungsgrundlage des § 38 Abs. 5 S. 1 BDSG nicht gedeckt sei. § 38 Abs. 5 S. 1 BDSG ermächtige zu Maßnahmen, die auf eine Veränderung eines Datenverarbeitungsvorganges bzw. auf Beseitigung von Mängeln innerhalb eines Datenverarbeitungsvorganges gerichtet seien. Die Untersagung eines Datenverarbeitungsvorganges oder gar die vollständige Beseitigung einer mit einem Datenverarbeitungsvorgang im Zusammenhang stehenden Infrastruktur könne gemäß § 38 Abs. 5 S. 1 BDSG nicht angeordnet werden. § 38 Abs. 5 S. 1 und 2 BDSG regelten die behördlichen Eingriffsbefugnisse im Bereich des Datenschutzes als gestuftes Verfahren. Erst bei Fruchtlosigkeit von Maßnahmen nach § 38 Abs. 5 S. 1 BDSG könne zu Maßnahmen nach § 38 Abs. 5 S. 2 BDSG (Untersagungsanordnungen) gegriffen werden. Dieses abgestufte Verfahren habe der Beklagte nicht eingehalten. Ohnehin sei ein Austausch der Ermächtigungsgrundlage (§ 38 Abs. 5 S. 2 BDSG statt § 38 Abs. 5 S. 1 BDSG) unzulässig.

Nur sie sei in der Lage, den Datenverarbeitungsvorgang zu modifizieren und insoweit sei die Klägerin nicht die richtige Adressatin für eine Anordnung nach § 38 Abs. 5 S. 1 BDSG. Die Tatsache, dass der Beklagte die streitige Anordnung an eine völlig ungeeignete Stelle richte, könne ihn jedoch nicht von der Notwendigkeit befreien, das in § 38 Abs. 5 S. 2 BDSG vorgesehene zweistufige Verfahren einzuhalten.

Die streitige Anordnung sei auch deshalb rechtswidrig, weil die Klägerin im Hinblick auf die Fanpage keine datenschutzrechtlich verantwortliche Stelle sei.

Adressat der Verpflichtungen in §§ 13, 15 TMG sei die datenschutzrechtlich verantwortliche Stelle gemäß § 12 Abs. 3 TMG iVm § 3 Abs. 7 BDSG und Art. 2 d) RL 95/46/EG. Fanpage-Betreiber seien keine datenschutzrechtlich verantwortliche Stelle, da sie nicht über Zwecke und Mittel der Datenverarbeitung (mit-)entscheiden würden. Die Datenverarbeitung für die Insights-Funktion laufe unbeeinflusst von den Betreibern einer Fanpage ab. Diese hätten keine Entscheidungsbefugnis in Bezug auf die Zwecke und Mittel der Datenverarbeitung. Die Möglichkeit, Nutzeraktivitäten auf einer Fanpage nachzuverfolgen, die Art der Verarbeitung der Daten und sogar, dass und wie diese aufbereitet und den

Fanpage-Betreibern zur Verfügung gestellt würden, habe sie unabhängig vom einzelnen Fanpage-Betreiber entschieden und in ihrer Infrastruktur angelegt. Der Entscheidungsspielraum der Fanpage-Betreiber beschränke sich einzig und allein auf die Frage, ob sie eine Fanpage anlegten oder nicht. Diese Entscheidung, eine Fanpage anzulegen, sei allein nicht als Entscheidung über die „Zwecke und Mittel der Verarbeitung von personenbezogenen Daten“ anzusehen. Im Sinne des Art. 2 d) RL 95/46/EG genüge gerade nicht jede Entscheidung, die entfernt ursächlich für das Ergebnis einer Datenverarbeitung sein könne. Vielmehr müsse die Entscheidungsbefugnis die Möglichkeit einräumen, die Datenverarbeitung selbst zu kontrollieren.

Das durch den Beklagten mit der Terminologie „gemeinsame Zwecksetzung“ suggerierte Zusammenwirken zwischen der Klägerin und ihr existiere nicht. Eine gemeinsame Zwecksetzung, wenn es sie denn tatsächlich gäbe, sei für eine gemeinsame Verantwortlichkeit ohnehin nicht ausreichend. Gemäß Art. 2 d) RL 95/46/EG sei nämlich die Entscheidung über „Zwecke und Mittel“ der Verarbeitung entscheidend, nicht über „Zwecke oder Mittel“. Die gemeinsame Zwecksetzung sei danach zwar eine notwendige, aber keine hinreichende Bedingung für das Vorliegen einer gemeinsamen Verantwortlichkeit. Auf die Mittel der Datenverarbeitung, insbesondere die im Netzwerk der Beigeladenen implementierte Insights-Funktion, habe die Klägerin aber keinen Einfluss.

Die Situation des Betreibers einer Fanpage im Netzwerk von Facebook sei nicht mit dem Betrieb einer Website im Internet vergleichbar. Eine Fanpage entstehe gerade nicht im Internet, sondern im (Parallel-)Netzwerk der Beigeladenen. Ein Fanpage-Betreiber habe daher keine mit dem Betreiber einer Website vergleichbaren Gestaltungs- oder Entscheidungsmöglichkeiten, sondern sei gezwungen, sich an die Spielregeln der Beigeladenen zu halten. Soweit Art. 2 d) RL 95/46/EG die Möglichkeit einer gemeinsamen datenschutzrechtlichen Verantwortung vorsehe, setze diese selbstverständlich voraus, dass jeder gemeinsam Verantwortliche selbst in Bezug auf die Datenverarbeitung oder zumindest Teilaspekte davon die Voraussetzung von Art. 2 d) RL 95/46/EG erfülle. Eine Gesamtverantwortung qua Zurechnung sehe Art. 2 d) RL 95/46/EG grundsätzlich nicht vor.

Es liege auch keine Auftragsdatenverarbeitung und keine einer Auftragsdatenverarbeitung vergleichbare Situation vor. Sie verarbeite keine personenbezogenen Daten im Auftrag der Klägerin. Ein Auftragsverhältnis mit einem Weisungsgehalt und der Möglichkeit der Kontrolle über die Datenverarbeitung existiere im Verhältnis zwischen der Klägerin und ihr nicht. Die Klägerin bestimme nicht die Zwecke der Datenverarbeitung, sondern profitiere lediglich vom Ergebnis einer eigenständig initiierten Datenverarbeitung der Beigeladenen. Auch die vom Beklagten konstruierte allgemeine Verantwortlichkeit vergleichbar einer „Störerhaftung“ könne die fehlende datenschutzrechtliche Verantwortung der Klägerin

nicht ersetzen. Die Figur einer Verantwortlichkeit für Störungszustände sei dem Datenschutzrecht fremd. Art. 2 d) RL 95/46/EG enthalte eine eigene explizite Regelung der datenschutzrechtlichen Verantwortlichkeit. Danach sei allein derjenige Verantwortliche im datenschutzrechtlichen Sinne, der eine Datenverarbeitung steuernd in den Händen halte, in dem er maßgeblich „über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheide“. Diese Definition der Verantwortlichkeit sei bei der Umsetzung der Datenschutzrichtlinie in nationales Recht nicht erweitert worden. Vielmehr sei § 3 Abs. 7 BDSG in Anlehnung an die Terminologie des Art. 2 d) RL 95/46/EG formuliert worden. Eine national-autonome Erweiterung auf „Nichtverantwortliche“ im Sinne der RL 95/46/EG sei also nicht beabsichtigt gewesen und wäre darüber hinaus europarechtlich unzulässig. Die Beigeladene ist im Übrigen der Auffassung, dass ihre Datenverarbeitung dem allein maßgeblichen irischen materiellen Datenschutzrecht entspreche. Im Übrigen sei die streitige Anordnung auch ermessensfehlerhaft.

Das Verwaltungsgericht hat durch Urteil vom 9. Oktober 2013 den Bescheid des Beklagten vom 3. November 2011 in der Fassung des Widerspruchsbescheides vom 16. Dezember 2011 aufgehoben und die Berufung zugelassen. In seiner Urteilsbegründung hat das Verwaltungsgericht entscheidungserheblich darauf abgestellt, dass die Klägerin datenschutzrechtlich nicht für die mit der Eröffnung einer Fanpage ausgelösten Vorgänge der Erhebung, Verwendung und Verarbeitung personenbezogener Daten von Nutzern der Fanpage durch Facebook (mit-)verantwortlich sei, auch wenn sie als Betreiberin einer Fanpage als Dienstanbieter im Sinne des § 2 Abs. 1 Nr. 1 TMG anzusehen sein dürfte.

Mit dem Begriff „Diensteanbieter“ im Sinne des Telemediengesetzes werde hinsichtlich der Bearbeitung personenbezogener Daten keine spezialgesetzliche Verantwortlichkeit abweichend von dem Begriff der verantwortlichen Stelle gemäß § 3 Abs. 7 BDSG bzw. Art. 2 d) der RL 95/46/EG (Datenschutzrichtlinie) geregelt.

Die Klägerin sei nicht verantwortliche Stelle im Sinne des § 3 Abs. 7 BDSG.

Im Hinblick auf die mit der Nutzung einer Fanpage ausgelöste Verarbeitung personenbezogener Daten durch Facebook könne weder von einer eigenen Datenverarbeitung durch die Klägerin noch davon gesprochen werden, dass diese die betreffende Datenverarbeitung durch die Beigeladene aufgrund eines Auftrages vornehmen lasse.

Der Nutzer der Fanpage der Klägerin bei Facebook rufe unmittelbar eine Facebook-Seite auf, so dass personenbezogene Daten ausschließlich vom Nutzer direkt zu Facebook gelangten. Insoweit unterscheide sich die Konstellation bei Fanpages von dem Fall, dass Anbieter von Online-Inhalten ihre Internetseite so konfigurieren, dass ein Besucher dieser

Seite automatisch zur Website des Betreibers eines Werbenetzwerkes umgeleitet wird, womit der Anbieter von Online-Inhalten die Übermittlung der IP-Adresse auslöse und hierfür den ersten erforderlichen Schritt zur Ermöglichung der folgenden Datenverarbeitung, die der Betreiber des Werbenetzwerkes ausübe, mache. Die Klägerin komme dagegen in keinerlei direkten Kontakt zu personenbezogenen Daten der Nutzer der Fanpage.

Dieser fehlende Kontakt schliesse ihre datenschutzrechtliche Verantwortlichkeit gemäß § 3 Abs. 7 BDSG und Art. 2 d) RL 95/46/EG nicht aus, wenn ein Fall der Auftragsdatenverarbeitung der Beigeladenen für die Klägerin im Sinne des § 11 Abs. 1 S. 1 BDSG vorläge. Dies sei jedoch nicht der Fall.

Die Beigeladene sei hinsichtlich der Erhebung, Verarbeitung und Nutzung personenbezogener Daten der Nutzer der Fanpage keine Auftragnehmerin der Klägerin. Ein Auftragsverhältnis zwischen der Klägerin und der Beigeladenen bestehe insoweit nicht. Es sei nicht feststellbar, dass insoweit in irgendeiner Weise eine vertragliche Beziehung zwischen der Klägerin und der Beigeladenen bestehe. Die vertragliche Beziehung sei für das Zurverfügungstellen der Fanpage durch die Beigeladene an die Klägerin entsprechend den Nutzungsbedingungen der Beigeladenen beschränkt. Die Erhebung, Verwendung und Verarbeitung personenbezogener Daten von Nutzern der Fanpage durch die Beigeladene sei nicht Gegenstand dieser Vereinbarung. Soweit die Beigeladene der Klägerin den kostenlosen Dienst „Insights“ zur Verfügung stelle, handele es sich lediglich um eine unabhängig von einem Auftrag ausgeführte statistische Auswertung der Nutzung der Fanpage mit dem Ergebnis von anonymisierten Statistikmaterial. Das für die Annahme eines Auftragsverhältnisses wesentliche Element eines vertraglichen Weisungsrechts fehle im Vertragsverhältnis der Klägerin und der Beigeladenen. Die Klägerin sei nicht „Herrin der Daten“.

Die Klägerin sei auch nicht verantwortliche Stelle gemäß § 3 Abs. 7 1. Alt. BDSG und Art. 2 d) RL 95/46/EG, da sie nicht „gemeinsam mit anderen“ über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden würde.

Es fehle der Klägerin sowohl hinsichtlich der Zwecke als auch der Mittel der Verarbeitung von personenbezogenen Daten der Nutzer der Fanpage an einer dieser allein oder gemeinsam mit der Beigeladenen zustehenden Entscheidungsgewalt. Die Zwecke und Mittel der Verarbeitung der betreffenden personenbezogenen Daten würden ausschließlich von der Beigeladenen bestimmt. Die Entscheidung der Klägerin beschränke sich auf die Annahme eines für sie unabänderlichen Angebots, die Fanpage einzurichten und mit Inhalten zu füllen oder nicht. Durch die Annahme dieses Angebots und die Errichtung einer

Fanpage bestimme die Klägerin nicht Zwecke und Mittel der Verarbeitung von personenbezogenen Daten der Nutzer der Fanpage.

Die datenschutzrechtliche Verantwortlichkeit in Bezug auf die Verarbeitung personenbezogener Daten richte sich ausschließlich nach der abschließenden Regelung in § 3 Abs. 7 BDSG, die im Lichte des Art. 2 d) RL 95/46/EG auszulegen sei. Eine Stelle, die weder einen rechtlichen noch einen tatsächlichen Einfluss auf die Entscheidung betreffend die Verarbeitung personenbezogener Daten habe, könne nicht als für die Verarbeitung Verantwortliche angesehen werden. Die Regelungen der Verantwortlichkeit in § 3 Abs. 7 BDSG und Art. 2 d) RL 95/46/EG könnten auch nicht durch einen Rückgriff auf Zurechnungsnormen des Privatrechts oder des allgemeinen Polizei- und Ordnungsrechts ausgeweitet werden.

Der Beklagte hat am 01. November 2013 die vom Verwaltungsgericht zugelassene Berufung gegen das ihm am 28. Oktober 2013 zugestellte Urteil eingelegt.

Der Beklagte wiederholt und vertieft seinen bisherigen Vortrag und führt zur Berufungsbeurteilung ergänzend aus:

Das Verwaltungsgericht erkenne die technischen Abläufe nur lückenhaft. Es habe nicht berücksichtigt, dass Facebook neben den genannten Cookies weitere Cookies setze. Vor diesem Hintergrund greife die Feststellung des Verwaltungsgerichts zu kurz, dass die eingesetzten Cookies einzig der Identifizierung von Mitgliedern und des Schutzes des Netzwerkes vor „böswilligen Aktivitäten“ dienten.

Für Facebook seien Fanpagebetreiber ein wichtiger Kooperationspartner, um Cookies zu verarbeiten. Die Fanpage-Angebote mit ihren Inhalten steigerten die Attraktivität des Netzwerkes für dessen Mitglieder. Vor allem aber lockten die dort präsentierten Inhalte Internetnutzer auf die von Facebook bereitgestellte Infrastruktur, die bislang keine Facebook-Mitglieder seien. Auch die Fanpagebetreiber profitierten von der Fanpage und setzen diese ein, obwohl sie wüssten, dass dadurch Profildaten der Nutzer zu Werbezwecken erhoben werden. Die Fanpage biete ihnen eine leistungsstarke Infrastruktur für die Vermarktung von Inhalten im Internet. An den im Rahmen des Netzwerkes erhobenen Nutzungsdaten partizipiere der Fanpagebetreiber unmittelbar. Er erhalte über die Funktion

„Facebook-Insights“ aussagekräftige Statistiken über die Besucher seiner Fanpage und könne so die Wirksamkeit seines Werbeauftritts in der Öffentlichkeit messen.

Das Verwaltungsgericht irre, wenn es meine, dass die Verantwortlichkeit der Klägerin als Auftragsdatenverarbeiter ausscheide, weil sie mit Facebook keinen wirksamen Vortrag im Sinne von § 11 Abs. 2 BDSG geschlossen habe. Der Vertrag im Sinne von § 11 Abs. 2 BDSG entscheide nicht über die Verantwortlichkeit. Das Vorliegen eines wirksamen Auftrages im Sinne von § 3 Abs. 2 BDSG taue allenfalls als Indiz dafür, wie die beteiligten Stellen die Verantwortlichkeit untereinander geteilt hätten. Der Vertrag sei Rechtsfolge des Auftrags.

Wann eine Stelle für die Einhaltung der Datenschutzvorschriften verantwortlich sei, regle nicht § 11 BDSG, sondern allein die allgemeine Definition aus § 3 Abs. 7 BDSG, die im Lichte von Art. 2 d) RL 95/46/EG auszulegen sei. Bei der Anwendung der Vorschrift verkenne das Verwaltungsgericht, dass die Klägerin als Fanpagebetreiberin sowohl über den Zweck als auch über die Mittel der Erhebung der Verarbeitung der Nutzungsdaten tatsächlich entscheide. Sie entscheide gemeinsam mit Facebook über den Zweck der Verarbeitung der Nutzungsdaten, indem sie ihre Fanpage angelegt habe und betreibe. Sie nutze die Fanpage für Werbezwecke und zur bedarfsgerechten Gestaltung ihrer angebotenen Telemedien. Die Zwecke könnten nicht auseinanderdividiert werden. Die Klägerin bezahle ihre öffentliche Präsentation mit den personenbezogenen Daten der Besucher der Fanpage. Die Klägerin entscheide auch über die Mittel der Datenverarbeitung im Sinne der Richtlinie. Dem stehe nicht entgegen, dass sie nicht unmittelbar auf die erhobenen Nutzungsdaten und die technischen Abläufe zugreifen könne. Die Entscheidung über die „Mittel“ müsse nicht die technischen Abläufe beinhalten, sondern einzig das „Wie“ der Datenverarbeitung. Während der Verantwortliche die technischen Details an einen Auftragsverarbeiter delegieren könne, trage die Verantwortung derjenige, der die „wesentlichen Elemente“ der Datenverarbeitung festlege. Diese Anforderung erfülle die Klägerin, da sie bewusst die Fanpage mit der darin enthaltenen „Insights-Funktion“ einsetze, zudem leisteten die Fanpagebetreiber durch das Erstellen von Inhalten einen wesentlichen Beitrag für die Erhebung und Verarbeitung der Nutzungsdaten. Die Auffassung, dass die Klägerin (mit-)verantwortliche Stelle im Sinne von Art. 2 b) und d) RL 95/46/EG sei, werde durch die Entscheidung des EuGH vom 13. Mai 2014 (C - 131/12) bestätigt. Der EuGH habe eine gemeinsame datenschutzrechtliche Verantwortlichkeit von Suchmaschinenbetreiber und Webseitenbetreiber für möglich gehalten, was zeige, dass an die Annahme einer gemeinsamen Verantwortlichkeit keine hohen Anforderungen gestellt werden dürften. Allein die technische Option, durch Aufschlussprotokolle oder Codes eine Indizierung

durch den Suchmaschinenbetreiber zu verhindern, könne daher zur Annahme einer datenschutzrechtlichen Verantwortlichkeit von Suchmaschinenbetreibern und Webseitenbetreibern führen, da diese gemeinsam über die verwendeten Mittel entscheiden würden. Führe bereits dieses Zusammenwirken zwischen Suchmaschinenbetreiber und Webseitenbetreiber zur Annahme einer gemeinsamen datenschutzrechtlichen Verantwortlichkeit, so treffe dies für die dargelegte Kooperation zwischen Facebook und der Klägerin erst recht zu. Zwischen Facebook und der Berufungsbeklagten bestehe eine vertragliche Vereinbarung zum Betrieb einer Fanpage.

Die vom Verwaltungsgericht vertretene Ansicht führe zu erheblichen Schutzlücken. Das Gericht verletze die gemäß Art. 8 EU-GrCH beziehungsweise Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG bestehende Schutzpflicht für das Recht auf informationelle Selbstbestimmung. Die Schutzdefizite müssten jedenfalls durch die Anwendung der Grundsätze der Störerhaftung geschlossen werden. Dem stehe weder Art. 2 d) RL 95/46/EG noch die vom Verwaltungsgericht zitierte Entscheidung des EuGH (Rechtsachen C - 468/10 und C - 469/10) entgegen, da diese den Harmonisierungsgrad der Richtlinie für die in Kapitel II der Richtlinie geregelten Erlaubnisgründe beträfen. Daraus könne nicht ohne Weiteres auf den vollharmonisierenden oder gar abschließenden Charakter der Richtlinie im Ganzen geschlossen werden. Auch der Zweck der Richtlinie zwingt dazu, dass neben der datenschutzrechtlichen Verantwortlichkeit Raum für die allgemeinen Grundsätze der Störerhaftung bleibe. Art. 1 Abs. 1 RL 95/46/EG verpflichte die Mitgliedsstaaten, den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten zu gewährleisten. Auch das BDSG gebe den für die Auslegung nötigen Raum, damit die Aufsichtsbehörden Anordnungen gegen die Störer treffen könnten. Aus dem Wortlaut des § 38 Abs. 5 BDSG folge jedenfalls nicht, dass die Behörde die Anordnung ausschließlich gegenüber verantwortlichen Stellen aussprechen dürfe. Aus dem Gesetzeszusammenhang ergebe sich zwar, dass Adressat der Maßnahmen die verantwortlichen Stellen sein können. Allein § 11 Abs. 4 S. 2 BDSG zeige aber, dass die Maßnahmen nicht allein an den Verantwortlichen, sondern auch an andere Stellen gerichtet sein könnten, wie etwa Auftragsdatenverarbeiter. Gemäß § 173 Abs. 1 LVwG führten Polizei- und Ordnungsbehörden wie das ULD zwar die Aufgabe der Gefahrenabwehr nach den besonderen Regelungen ihres jeweiligen Ordnungsrechts durch. Soweit diese aber fehlten und eine abschließende Regelung nicht enthielten, würden die allgemeinen Regeln des Gefahrenabwehrrechts aus den §§ 174 - 227 LVwG, § 173 Abs. 2 LVwG gelten. Die Klägerin erfülle mit ihrem Verhalten die Voraussetzung für die Inanspruchnahme als Zweckveranlasser, da Facebook datenschutzrechtliche Nutzungsdaten verarbeite und die Berufungsbeklagte

mit dem Betrieb der Fanpage einen Beitrag leiste, der mit der Störung eine natürliche Handlungseinheit bilde. Mit dem Dienst „Facebook-Insights“ verstoße Facebook gegen geltendes Datenschutzrecht. Dabei könne dahinstehen, ob die Handlungen des Netzbetreibers nach § 1 Abs. 5 S. 2 BDSG dem deutschen oder gemäß § 1 Abs. 5 S. 1 BDSG dem irischen Datenschutzrecht unterlägen. Richtig sei allerdings, dass Facebook Inc. deutsches Datenschutzrecht, insbesondere die Regelungen des TMG, beachten müsse, denn Facebook Inc. betreibe in Deutschland mit der Facebook Germany GmbH eine Niederlassung im Sinne von Art. 4 Abs. 1 a) der RL 95/46/EG. Deutsches Datenschutzrecht sei jedenfalls anwendbar, weil die amerikanische Facebook-Konzernmutter in Deutschland personenbezogene Daten verarbeite und die Anwendung deutschen Datenschutzrechts nicht gemäß § 1 Abs. 5 S. 1 1. HS BDSG durch irisches Datenschutzrecht ausgeschlossen werde.

Der Beklagte beantragt,

das verwaltungsgerichtliche Urteil zu ändern und die Klage abzuweisen.

Die Klägerin beantragt,

die Berufung zurückzuweisen.

Sie erwidert:

Die Ausführungen des Beklagten zur lückenhaften technischen Bewertungsgrundlage des Verwaltungsgerichts entbehrten jeglicher Substanz. Er beschränke seinen Vortrag auf „erhebliche Zweifel“ an den Ausführungen und Erklärungen von Facebook zu Art, Umfang und Erforderlichkeit eingesetzter Cookies. Es sei nicht dargelegt und nicht ersichtlich, mit welchen Cookies und durch welche Handlungen genau Facebook gegen datenschutzrechtliche Bestimmungen verstoße. Die für Facebook zuständige Datenschutzbehörde in Irland komme zum Ergebnis der Datenschutzkonformität von Facebook.

Unberücksichtigt bleibe auch die vom Beklagten selbst zu Recht angeführte Möglichkeit eines jeden Nutzers der Plattform, durch entsprechende Browsereinstellungen die Annahme von Cookies schon vor Verwendung etwaiger Onlinedienste zu unterbinden. Unberücksichtigt bleibe des Weiteren das Informationsangebot von Facebook, das jedem

Nutzer die Möglichkeit biete, sich schon vor der Registrierung über datenschutzrechtliche Aspekte auf der Plattform „Facebook“ zu informieren.

Die Klägerin sei falsche Adressatin der Anordnung. Sie bediene sich schlicht einer vorgegebenen Infrastruktur. Sie nutze diese genauso wie die User, welche die Fanpage der Klägerin aufrufen. Der Beklagte möge sich insoweit an den Betreiber von „Facebook“ wenden und sich gegebenenfalls mit der irischen Datenaufsicht ins Benehmen setzen.

Im Übrigen erschöpften sich die Ausführungen des Beklagten in nicht näher substantiierten Mutmaßungen mit Blick auf mögliche Datennutzungen durch Facebook, die über das Erforderliche hinausgingen. Tatsächliche Anhaltspunkte stützten diese Mutmaßungen nicht. Schlicht falsch sei in diesem Zusammenhang die Darstellung des Beklagten, Fanpagebetreiber seien für Facebook „Kooperationspartner, um Cookies zu verbreiten“. Richtig sei allein, dass Facebook eine technische Infrastruktur zur Verfügung stelle, die sowohl Betreiber von sogenannten Fanpages als auch deren Besucher nutzten, um sich auf dieser zur Verfügung gestellten Infrastruktur zu treffen. Ohne den als selbstverständlich vorausgesetzten Betrieb einer entsprechenden Fanpage sähe sich die Klägerin erheblichen Wettbewerbsnachteilen im Vergleich zu denjenigen Unternehmen ausgesetzt, die eine entsprechende Fanpage betreiben und auf dem Medium „Facebook“ sichtbar seien. Es gehe nicht um Kostenersparnisse, sondern allein um eine dem Markt geschuldete angemessene Sichtbarkeit im digitalen Umfeld.

Eine Auftragsdatenverarbeitung komme in der Konstellation Fanpage - Nutzer / Facebook unter keinem rechtlichen oder tatsächlichen Gesichtspunkt in Betracht. Es fehle nicht nur an entsprechenden Vereinbarungen, vielmehr liege bereits im Ausgangspunkt konstruktiv auch keine mit der Auftragsdatenverarbeitung vergleichbare Ausgangslage vor. Die Klägerin habe Facebook nicht mit der Verarbeitung irgendwelcher Daten beauftragt. Die Beklagte unterhalte lediglich ein Nutzungsverhältnis mit Facebook, das es ihr ermögliche, eine Fanpage auf der von Facebook zur Verfügung gestellten Infrastruktur zu betreiben. Sie habe gar kein Interesse daran, dass Facebook irgendwelche Daten erhebe. Wenn und soweit Facebook Daten erhebe, erfolge dies jedenfalls nicht auf Veranlassung oder im Auftrag der Klägerin. Kennzeichen für eine Auftragsdatenverarbeitung im Sinne des § 11 BDSG sei, dass Daten vom Auftragsdatenverarbeiter für einen Auftraggeber im Sinne des Auftraggebers nach Weisungen des Auftraggebers so erhoben werden, dass es sich bei den erhobenen Daten ausschließlich um solche des Auftraggebers und nicht des Auftragsnehmers handele. Vorliegend habe die Klägerin jedoch überhaupt keine Kenntnis von irgendwelchen Daten, die gegebenenfalls von Facebook erhoben werden. Sie entscheide auch nicht gemeinsam mit Facebook über den Zweck der Verarbeitung der Nut-

zungsdaten. Sie erhebe keine Nutzungsdaten. Soweit Facebook Daten von Nutzern erhebe und diese Nutzungsdaten zudem im Zusammenhang mit der von der Klägerin betriebenen Fanpage stehen sollten, was nach wie vor offen sei, handele es sich hierbei allein um Handlungen von Facebook. Diese Handlungen würden weder von der Klägerin unterstützt, noch liege dem gar ein gemeinsamer Entschluss der Beklagten mit Facebook zugrunde. Auch die immer wieder zitierte Facebook - Funktionalität „Facebook-Insights“ führe nicht zu einer anderen rechtlichen Beurteilung. Niemand nutze Facebook wegen „Insights“. Bei der entsprechenden Funktionalität, aufgrund derer anonymisierte Nutzerstatistiken zur Verfügung gestellt werden, handele es sich schlicht um einen „nicht abstellbaren Service“ von Facebook als Infrastrukturanbieter. Ihr fehle das für die Begründung einer eigenen Verantwortlichkeit erforderliche Bestimmungsrecht über die von Besuchern von der Fanpage von Facebook erhobenen Daten. Das Bestimmungsrecht liege ausschließlich bei Facebook. Dies sei auch ohne Weiteres für den durchschnittlichen Facebook - Nutzer erkennbar.

Einen nicht verantwortlichen Dritten als Instrument zu gebrauchen, um mittelbar gegen einen verantwortlichen Betreiber vorzugehen, der zudem nach Überzeugung der für ihn zuständigen irischen Datenschutzaufsicht in Übereinstimmung mit den anwendbaren und vereinheitlichten Datenschutzgesetzen handele, unterfalle keinesfalls dem Gebot effektiven Grundrechtsschutzes.

Die vom Beklagten vorgebrachte „Schutzlückenargumentation“ verfange nicht. Es bestehe schon kein Schutzbedürfnis. Träfen sich zwei Nutzer (Betrachter der Fanpage und Betreiber der Fanpage) auf einem gemeinsamen von beiden gewählten Medium, so unterlägen beide Nutzer den gleichen Regelungen / Einschränkungen, die durch den Plattformanbieter (Facebook) vorgegeben würden. Ein Schutzbedürfnis könne insoweit nur im Verhältnis vom Nutzer zu Facebook, nicht jedoch im Verhältnis Nutzer / Nutzer bestehen. § 3 Abs. 7 BDSG und Art. 2 d) RL 95/46/EG trafen abschließende Regelungen bezüglich der datenschutzrechtlichen Verantwortlichkeit. Ein etwaiger Rückgriff auf eine - wie auch immer geartete - Störerhaftung sei mithin ausgeschlossen. Neben Art. 2 d) ergebe sich schon aus Art. 23 RL 95/46/EG eine jedenfalls mit Blick auf die datenschutzrechtliche Verantwortlichkeit abschließende Regelung. Der Artikel stelle insoweit die Grundlage der Schadensersatzhaftung der Richtlinie dar. Art. 23 Abs. 1 RL 95/46/EG setze als Haftungsgrund gerade eine rechtswidrige Verarbeitung der Daten voraus. Im Zusammenhang des Kriteriums „rechtswidrige Verarbeitung“ mit dem in Art. 23 Abs. 1 RL 95/46/EG benannten Passivlegitimierten als „für die Verarbeitung Verantwortlichem“ folge, dass nach dem Wil-

len des europäischen Gesetzgebers eine Aufteilung zwischen „Rechtswidrigkeit“ und „Verantwortlichkeit“ nicht möglich sei.

Selbst wenn man entgegen der Richtlinie 95/46/EG und entgegen den tatsächlichen Sachverhaltsgegebenheiten von der grundsätzlichen Anwendbarkeit entweder der Störerhaftung oder der Zweckveranlasserhaftung ausgehe, ändere dies nichts am Ergebnis. Für die Annahme eines zivilrechtlichen Störers fehle es an einem willentlichen bzw. adäquat kausalen Beitrag durch die Beklagte zu einer unterstellt rechtswidrigen Datenverarbeitung durch Facebook. Zwischen der Klägerin und Facebook bestehe kein Wirkungs- und Verantwortungszusammenhang oder eine Kooperation. Auch unterfalle die Klägerin nicht der Definition eines Zweckveranlassers im öffentlich-rechtlichen Sinne. Facebook handele nicht auf Veranlassung eines Nutzers, sondern stelle jedem Nutzer der Facebook Plattform die entsprechenden Kapazitäten / Infrastrukturen zur Verfügung. Ebenso wenig wie eine Auftragsdatenverarbeitung vorliege, liege eine Veranlassung der Beklagten gegenüber Facebook mit Blick auf die Vornahme irgendwelcher rechtswidriger Handlungen vor. Es fehle insoweit offensichtlich an jeglichem subjektiven Element.

Die Klägerin unterfalle schließlich auch nicht den Regelungen des § 15 Abs. 3 TMG, wie das Verwaltungsgericht festgestellt habe. Auch könne der Klägerin schon ein Verstoß gegen § 15 Abs. 3 TMG nicht vorgeworfen werden, weil sie überhaupt keine Daten im Sinne der Vorschrift verarbeite.

Die Beigeladene beantragt,

die Berufung zurückzuweisen.

Sie legt zunächst dar, dass sie für die Facebook-Nutzer außerhalb Nordamerikas zuständig sei, schildert das Vorgehen bei Abschluss von Nutzungsverhältnissen, die Funktionalität von Fanpages sowie der Insights-Funktion und führt dann wiederholend und vertiefend im Einzelnen aus, dass die streitige Anordnung des Beklagten an zahlreichen formellen und materiellen Mängeln leide. Sie sei formell rechtswidrig, weil sie auf die falsche Rechtsgrundlage des § 38 Abs. 5 S. 1 BDSG gestützt sei und das in § 38 Abs. 5 BDSG vorgesehene zweistufige Verfahren nicht eingehalten sei. In materieller Hinsicht sei die streitige Anordnung nicht von einer Ermächtigungsgrundlage gedeckt. Darüber hinaus richte sich die streitige Anordnung an die falsche Adressatin, die Klägerin sei für die vom Beklagten kritisierte Insights-Funktion keine datenschutzrechtlich verantwortliche Stelle.

Der Beklagte könne die Klägerin auch nicht als Störer in Anspruch nehmen. Ein Verstoß gegen datenschutzrechtliche Vorschriften liege nicht vor. Schließlich habe der Beklagte, selbst wenn man vom Vorliegen der Voraussetzungen zum Erlass der streitigen Anordnung ausgehen wollte, sein Ermessen beim Erlass der streitigen Anordnung in mehrfacher Hinsicht fehlerhaft ausgeübt.

Wegen der weiteren Einzelheiten des Sachverhalts und des übrigen Vorbringens der Beteiligten wird auf die eingereichten Schriftsätze der Beteiligten sowie den Verwaltungsvorgang des Beklagten, der Gegenstand der mündlichen Verhandlung war, Bezug genommen.

Entscheidungsgründe:

Die zugelassene und auch im Übrigen zulässige Berufung ist nicht begründet.

Das Verwaltungsgericht hat zutreffend entschieden, dass der Bescheid des Beklagten vom 3. November 2011 in der Fassung des Widerspruchsbescheides vom 16. Dezember 2011 rechtswidrig ist und die Klägerin in ihren Rechten verletzt.

Mit Bescheid vom 3. November 2011 hat der Beklagte angeordnet, dass die Klägerin die von ihr betriebene Fanpage bei Facebook zu deaktivieren habe, weil Facebook gegen datenschutzrechtliche Vorschriften, insbesondere gegen § 15 Abs. 5 TMG, verstoße.

Als Rechtsgrundlage für die Anordnung kommt allein § 38 Abs. 5 BDSG in Betracht. Die Anordnung ist auch auf der Grundlage dieser Vorschrift ergangen. Das TMG enthält keine Ermächtigungsgrundlage. Nach § 59 Abs. 1 des Staatsvertrages für Rundfunk und Telemedien überwachen die nach den allgemeinen Datenschutzgesetzen des Bundes und der Länder zuständigen Kontrollbehörden für ihren Bereich die Einhaltung der Datenschutzbestimmungen des TMG. In Ermangelung einer spezialgesetzlichen Regelung im TMG richtet sich die zuständige Aufsichtsbehörde für Telemediendiensteanbieter nach § 38 BDSG. Nach § 39 Abs. 3 LDSG ist der Beklagte die zuständige Aufsichtsbehörde für

nicht-öffentliche Stellen nach § 38 BDSG. Zur Gewährleistung der Einhaltung unter anderem der Vorschriften des TMG kann er gemäß § 38 Abs. 5 BDSG Maßnahmen anordnen.

Der streitgegenständliche Bescheid ist bereits deshalb rechtswidrig, weil § 38 Abs. 5 BDSG die konkret getroffene Anordnung der Deaktivierung der Fanpage der Klägerin nicht trägt.

Nach § 38 Abs. 5 S. 1 BDSG kann die Aufsichtsbehörde Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten (nachfolgend Datenverarbeitung) oder technischer oder organisatorischer Mängel anordnen. Nach S. 2 kann selbst bei schwerwiegenden Verstößen und Mängeln die Datenverarbeitung als solche oder der Einsatz einzelner Verfahren erst untersagt werden, wenn die Verstöße oder Mängel entgegen der Anordnung nach S. 1 und trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden. Die Vorschrift schreibt mithin ein abgestuftes Verfahren vor. Bevor ein Datenverarbeitungsverfahren untersagt werden kann, muss die Aufsichtsbehörde die datenverarbeitende Stelle auffordern, Maßnahmen zur Beseitigung von Rechtsverstößen zu ergreifen. Mit der Anordnung der Deaktivierung der Fanpage der Klägerin soll die Verarbeitung von Daten der Besucher der Fanpage (durch Facebook) über die sogenannte Insights-Funktion ausgeschlossen werden. Die angeordnete Maßnahme kommt daher der Untersagung der Datenverarbeitung als solcher gleich und geht noch darüber hinaus. Der Klägerin wird nicht nur die Datenverarbeitung untersagt, sondern die Teilnahme an einer Infrastruktur. Jedenfalls lässt die Anordnung der Klägerin nicht den Raum, datenschutzrechtliche Verstöße abzustellen.

Dem Untersagungscharakter der Anordnung steht nicht entgegen, dass die Klägerin unternehmensintern die Fanpage weiter nutzen und die Inhalte im Rahmen anderer Dienste verwenden kann. Sinn und Zweck der Fanpage ist, mit Interessierten über diese Infrastruktur zu kommunizieren. Das wird durch die Deaktivierung unmöglich gemacht. Dass die Klägerin andere Dienste in Anspruch nehmen kann, ist ebenso eine Selbstverständlichkeit wie die Fortsetzung einer Datenverarbeitung nach Beseitigung von datenschutzrechtlichen Verstößen.

Die Vorschrift des § 38 Abs. 5 BDSG sieht keine Ausnahme vom abgestuften Verfahren vor. Ungeachtet des Wortlauts können aber Ausnahmen gerechtfertigt sein (noch offen

gelassen vom Senat im Beschluss v. 12.01.2011 - 4 MB 56/10 -, NordÖR 2011, 501). Voraussetzung ist, dass ein Datenverarbeitungsverfahren nicht nur unter einzelnen Gesichtspunkten mangelhaft, sondern - etwa wegen Fehlens einer Rechtsgrundlage - in seiner Gesamtheit unzulässig ist und dieser Mangel nur durch die Einstellung des Verarbeitungsverfahrens beseitigt werden kann (so Gola/Schomerus, BDSG, 11. Aufl., § 38 Rn. 26) bzw. die Unmöglichkeit der Fehlerbeseitigung von vornherein feststeht (so Petri in Simitis, BDSG, 7. Aufl., § 38 Rn. 73). In Anbetracht des Wortlauts der Regelung des § 38 Abs. 5 BDSG sind die Ausnahmen aber eng zu begrenzen. Eine Abweichung vom Wortlaut ist nur dann gerechtfertigt, wenn die Einhaltung des abgestuften Verfahrens objektiv sinn- und zwecklos erscheint. Dies ist vorliegend nicht der Fall.

Die vom Beklagten behaupteten Verstöße könnten von Facebook ohne Weiteres beseitigt werden. Unabhängig davon, ob im Verhältnis zu Facebook materielles deutsches oder irisches Datenschutzrecht anzuwenden ist (s. hierzu Beschl. d. Senats v. 22.04.2013 - 4 MB 11/13 -, NJW 2013, 1977 aber auch KG Berlin, Urt. v. 24.01.2014 - 5 U 42/12 -, K & R 2014, 208 sowie EuGH Urt. v. 13.05.2014 - C - 131/12 -, Juris), bleiben die Zuständigkeiten der Aufsichtsbehörde unberührt. Insbesondere folgt aus der Anwendung materiellen irischen Datenschutzrechtes kein Eintritt der irischen Aufsichtsbehörde. Dies ergibt sich aus § 1 Abs. 5 S. 5 BDSG, wonach § 38 Nr. 1 S. 1 BDSG unberührt bleibt (s. Dammann in Simitis, a.a.O., § 1 Rn. 239). Das Vorgehen gegen Facebook wäre auch deutlich effektiver. Auf diese Weise könnten vom Beklagten, seine Zuständigkeit unterstellt, datenschutzrechtliche Verstöße von Facebook infolge des Betriebes von Fanpages in Schleswig-Holstein beseitigt werden, unabhängig davon, ob Fanpages von öffentlichen oder nicht-öffentlichen Stellen betrieben werden. Dies gilt insbesondere dann, wenn - wie der Beklagte unter Berufung auf die Entscheidung des EuGH (Urt. v. 13.05.2014, a.a.O.) und das Urteil des Kammergerichts Berlin (Urt. v. 24.01.2014, a.a.O.) meint - für Facebook, soweit personenbezogene Daten im Inland erhoben werden, materielles deutsches Datenschutzrecht gilt und damit von Facebook auch die Regelungen des TMG zu beachten sind. Ist das nicht der Fall, kommt es auf die Regelungen des TMG von vornherein nicht an. Dann kommen aber insoweit auch keine datenschutzrechtlichen Verstöße vor, die der Klägerin zugerechnet werden könnten. Anderes gilt nur, wenn sie „Herrin der Daten“ ist, dem TMG als Diensteanbieterin unterliegt und eigenverantwortlich gegen Regelungen des TMG verstößt. Dann ist aber ihr gegenüber auch das abgestufte Verfahren des § 38 Abs. 5 BDSG einzuhalten. Davon kann nicht abgesehen werden, weil ihr von Facebook nicht die technische Möglichkeit bereitgestellt wird, die Besucher ihrer Fanpage von einer Wi-

derspruchsmöglichkeit zu unterrichten. Als „Herrin der Daten“ wäre sie gegenüber Facebook weisungsberechtigt und könnte auf diesem Wege die festgestellten datenschutzrechtlichen Verstöße beseitigen. Sollte der Beklagte nicht die für Facebook zuständige Kontrollstelle sein, obwohl sich die Tätigkeit von Facebook auch auf Schleswig-Holstein erstreckt, was keiner abschließenden Entscheidung bedarf, kann er deshalb nicht anstelle von Facebook, abweichend vom vorgeschriebenen Verfahren, einen Dritten im Sinne des Art. 2 f) der RL 95/46/EG belangen.

Des Weiteren ist die Anordnung rechtswidrig, weil die Klägerin keine verantwortliche Stelle im Hinblick auf die von Facebook erhobenen Daten infolge des Betriebes ihrer Fanpage im Sinne des § 3 Abs. 7 BDSG bzw. im Sinne des Art. 2 d) der RL 95/46/EG ist und eine Anordnung nach § 38 Abs. 5 BDSG nur gegenüber der verantwortlichen Stelle ergehen kann.

Die Klägerin ist Diensteanbieterin im Sinne des § 2 Nr. 1 TMG, weil sie als Betreiberin einer Fanpage ein Telemedium zur Nutzung bereithält. Der Diensteanbieter ist jedoch nach dem Wortlaut der Regelungen der §§ 11 ff. TMG lediglich für die eigene Erhebung und Verwendung personenbezogener Daten verantwortlich.

Nach § 12 Abs. 3 TMG findet § 3 Abs. 7 BDSG Anwendung, weil das TMG nichts anderes bestimmt. Davon geht auch der Beklagte aus.

Gemäß § 3 Abs. 7 1. Alt. BDSG ist verantwortliche Stelle jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt. Die Klägerin erhebt und verarbeitet keine personenbezogenen Daten der Besucher der Fanpage für sich selbst. Der Beklagte stützt seine Anordnung auch allein auf die Erhebung und Verarbeitung von Daten durch Facebook. Die Klägerin übermittelt auch keine Daten an Facebook. Übermitteln ist gemäß § 3 Abs. 4 S. 2 Nr. 3 BDSG die Bekanntgabe gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten. Facebook ist kein Dritter in diesem Sinne. Die Fanpage ist eine Facebook-Seite. Es ist die Beigeladene, die bei Aufruf einer Fanpage über ihr Netzwerk unmittelbar die IP-Adresse des Nutzers erhält und auf dem Computer des Nutzers Cookies hinterlegt. Anhand der Cookies kann die Beigeladene ihre Nutzer erkennen und die Aktivität auf der Fanpage mit

den sonstigen Informationen verknüpfen, die sie über den jeweiligen Nutzer hat. Schon allein deshalb, weil die Klägerin selbst keine Daten von Nutzern erhebt, ist sie keine verantwortliche Stelle im Sinne des § 3 Abs. 7 1. Alt. BDSG.

Aus Art. 2 d) der RL 95/46/EG folgt nichts anderes. Danach ist „für die Verarbeitung Verantwortlicher“ jede Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Datenschutzrechtliche Verantwortlichkeit und Datenverarbeitung stehen danach ebenfalls in einem untrennbaren Zusammenhang. Die Klägerin trifft keine Entscheidung bezüglich der Verarbeitung von personenbezogenen Nutzerdaten durch Facebook. Insbesondere entscheidet sie nicht gemeinsam über die Zwecke und Mittel der Verarbeitung. „Zweck“ ist „das erwartete Ergebnis, das beabsichtigt ist oder die geplante Aktion leitet“ (Art. 29 - Datenschutzgruppe - WP 169, S. 16). Der Zweck der Erhebung und der Verarbeitung von personenbezogenen Nutzerdaten durch Facebook ist, die Wirtschaftlichkeit des Unternehmens Facebook zu steigern. Darauf weist auch der Beklagte hin, wenn er betont, dass die von Facebook gesetzten Cookies eine zentrale Rolle für das Geschäftskonzept von Facebook spielen. Im Rahmen der sogenannten „Insights - Funktion“ erhalten Fanpagebetreiber (ungefragt) anonymisierte und aggregierte Informationen über Nutzeraktivitäten auf ihrer Fanpage. Facebook verfolgt damit den weiteren Zweck, dass die Fanpagebetreiber ihre Page möglichst attraktiv gestalten, um auf diese Weise - mit den Worten des Beklagten - weitere Nutzer auf die von Facebook betriebene Infrastruktur zu locken. Auch die Fanpagebetreiber sind sicherlich daran interessiert, dass ihre Seiten für Nutzer attraktiv sind. Deshalb dürfte auch für die Klägerin ein Feedback von Facebook über Nutzeraktivitäten auf ihrer Fanpage nicht unwillkommen sein. Der Zweck des Betreibens einer Fanpage ist für sie aber nicht der Erhalt dieser Informationen, sondern mit Interessierten zu kommunizieren. Die Zwecke sind zu unterscheiden. Der Fanpagebetreiber entscheidet nicht über den Zweck, dass heißt das „Warum“ der Verarbeitung von personenbezogenen Daten zusammen mit Facebook, vielmehr bestimmt Facebook diesen Zweck allein. Der Fanpagebetreiber nutzt womöglich die im Rahmen der Insights-Funktion erhaltenen, anonymisierten Informationen, um allgemein besser mit Nutzern „ins Gespräch“ zu kommen. Er nutzt aber keine personenbezogenen Daten im Sinne des § 3 Abs. 5 BDSG, sondern gegebenenfalls Statistiken, die ihm Facebook aus eigenen Zwecken ungefragt zur Verfügung stellt.

Erst recht entscheidet der Fanpagebetreiber nicht über die Mittel zur Erreichung dieses Zweckes. „Mittel“ bezeichnet die „Art und Weise, wie ein Ergebnis oder Ziel erreicht wird“ (Art. 29 - Datenschutzgruppe, a.a.O.). Über das „Wie“ entscheidet Facebook ebenfalls allein. Die Fanpagebetreiber haben darauf keinerlei Einfluss. Der Fanpagebetreiber entscheidet nur, „ob“ er eine Fanpage einrichtet und betreibt. Das macht ihn aber nicht zum „für die Verarbeitung Verantwortlichen“. Eine Stelle, die weder einen rechtlichen noch einen tatsächlichen Einfluss auf die Entscheidung hat, wie personenbezogene Daten verarbeitet werden, kann nicht als für die Verarbeitung Verantwortliche angesehen werden (Art. 29 - Datenschutzgruppe - WB 169, S. 15).

Entscheidend für die Frage, ob mehrere Stellen gemeinsam für die Datenverarbeitung Verantwortliche sind, ist die Kontrolle und die Einflussnahmemöglichkeit auf die Datenverarbeitung. Diese fehlt dem Fanpagebetreiber vollständig. Er schafft zwar mit der Einrichtung und dem Betreiben einer Fanpage die unerlässliche Voraussetzung dafür, dass Facebook personenbezogene Daten über diese Page von Besuchern erheben kann, „ob“, „warum“ und „wie“ die Datenverarbeitung erfolgt, entscheidet dagegen Facebook allein.

Eine Vergleichbarkeit mit Anbietern von Online-Inhalten, die unter anderem Platz auf ihrer Website vermieten, damit Werbenetzwerke über Cookies ihre Werbung platzieren können (s. hierzu Art. 29 - Datenschutzgruppe WP 171, S. 13), ist nicht gegeben. Hierzu hat das Verwaltungsgericht bereits das Erforderliche gesagt. Der Fanpagebetreiber entscheidet nicht darüber, ob Facebook die Möglichkeit erhält, anlässlich des Besuchs einer Fanpage Cookies auf dem Computer der Nutzer zu Werbezwecken zu setzen, vielmehr befindet sich der Nutzer, wenn er eine Fanpage aufruft, bereits im Netzwerk und auf einer Seite von Facebook. Ohne dass es einer Entscheidung des Fanpagebetreibers bedarf, wird Facebook die IP-Adresse der Nutzer durch das Netzwerk übermittelt und werden Cookies gesetzt, um Informationen über die Nutzer zu erhalten und mit vorhandenen Informationen zu verknüpfen, um auf diese Weise für die Nutzer die Attraktivität des Netzwerkes zu steigern, vor allem aber um Werbeanzeigen und sonstige kommerzielle bzw. gesponserte Inhalte Nutzern zur Verfügung zu stellen.

Auch auf das Urteil des EuGH vom 13. Mai 2014 (a.a.O.) lässt sich die Auffassung des Beklagten, dass die Klägerin gemeinsam mit Facebook die datenschutzrechtliche Verantwortung für die von Facebook durchgeführte Datenverarbeitung trägt, nicht stützen. Der

EuGH hat festgestellt, dass Google Inc., soweit Google das Internet automatisch, kontinuierlich und systematisch auf dort veröffentlichte Informationen durchforstet, personenbezogene Daten im Sinne des Art. 2 b) RL 95/46/EG verarbeitet, die verantwortliche Stelle gemäß Art. 2 d) der Richtlinie ist. Des Weiteren hat der EuGH festgestellt, dass die Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeit einer Suchmaschine ausgeführt wird, sich von der unterscheidet, die von den Herausgebern von Websites, die diese Daten auf einer Internetseite einstellen, vorgenommen wird und zusätzlich zu dieser erfolgt. Es handelt sich mithin um zwei unterschiedliche Datenverarbeitungen und damit auch unterschiedliche Verantwortlichkeiten. Schließlich hat der EuGH ausgeführt, dass an der Verantwortung von Google der Umstand, dass die Herausgeber von Websites die Möglichkeit hätten, den Suchmaschinenbetreibern zu signalisieren, dass eine bestimmte auf ihrer Website veröffentlichte Information ganz oder teilweise von den automatischen Indexen der Suchmaschine ausgeschlossen werden solle, an der Verantwortlichkeit von Google nichts ändere. Eine Vergleichbarkeit mit dem vorliegenden Fall besteht nicht. Anders als Google erhebt und verarbeitet die Klägerin keine Daten. Insbesondere ging es in der Entscheidung des EuGH nicht um eine gemeinsame, sondern getrennte Verantwortlichkeit.

Die Klägerin ist auch nicht datenverarbeitende Stelle, weil sie Daten durch andere (Facebook) in ihrem Auftrag verarbeiten lässt (§ 3 Abs. 7 2. Alt. BDSG).

Die Klägerin hat die Beigeladene nicht mit der Erhebung von personenbezogenen Daten der Besucher ihrer Fanpage im Sinne des § 3 Abs. 7 2. Alt. BDSG beauftragt. Eine Auftragsdatenverarbeitung ohne Auftrag gibt es nicht. Die Auftragsdatenverarbeitung ist dadurch gekennzeichnet, dass der Auftraggeber die von ihm gewünschte Datenverarbeitung nicht selbst durchführt, sondern dies einem anderen (dem Auftragnehmer) überlässt. § 3 Abs. 7 2. Alt. BDSG stellt klar, dass die Verantwortlichkeit einer Person oder Stelle nicht davon abhängt, ob er die Daten selbst verarbeitet oder sich eines Auftragsverarbeiters bedient. Er bleibt verantwortliche Stelle. Dieses Prinzip liegt auch den speziellen Regelungen des § 11 Abs. 1 BDSG für die Datenverarbeitung im Auftrag zugrunde (Dammann a.a.O., § 3 Rn. 227). Der Auftraggeber, der den Zweck der Datenverarbeitung bestimmt, dem Auftragnehmer aber die Datenverarbeitung überlässt, wird gemäß § 11 Abs. 1 BDSG nicht aus der Verantwortung entlassen, obwohl er selbst (womöglich) gar nicht in den Besitz der Daten gelangt und auch nicht die physische Herrschaft über den Verarbeitungsprozess besitzt, weil er als Auftraggeber die Datenverarbeitung steuert und dem Auftrag-

nehmer Weisungen erteilen kann und muss, mithin Herr der Daten auch bei Auslagerung der Datenverarbeitung bleibt. Dies bedeutet allerdings nicht, dass der Auftragsverarbeiter nicht auch verantwortliche Stelle ist, seine Verantwortung ist eingeschränkt und nicht ausgeschlossen (Dammann, a.a.O., Rn. 228). Der Inhalt des nach § 11 Abs. 2 S. 2 BDSG schriftlich zu erteilenden Auftrags ist Ausgangspunkt für die Abgrenzung der Verantwortlichkeiten. Durch die Schriftform soll erreicht werden, dass der Auftraggeber auch tatsächlich Weisungen erteilt und der Auftragnehmer nachweisen kann, dass er weisungsgemäß verfahren ist (Gola/Schomerus, a.a.O., § 11 Rn. 17). Enthält der Vertrag klare Regelungen in Bezug auf den für die Verarbeitung verantwortlichen und weisungsberechtigten Auftraggeber und gibt es keinen Grund zu bezweifeln, dass diese die Realität korrekt widerspiegeln, ist die datenschutzrechtliche Verantwortlichkeit danach zu beurteilen. Wird der Vertrag nicht gelebt, weil der Auftragnehmer tatsächlich entscheidet, wie personenbezogene Daten verarbeitet werden, und kann der Auftraggeber keine Kontrolle ausüben, liegt faktisch ungeachtet des Auftrags keine Auftragsdatenverarbeitung vor; vielmehr ist dann der Auftragnehmer die maßgeblich verantwortliche Stelle, selbst wenn der Vertrag die Einstufung des (angeblichen) Auftragnehmers als für die Verarbeitung Verantwortlicher ausdrücklich ausschließt (s. hierzu Art. 29 - Datenschutzgruppe WP 169 S. 14). Dies bedeutet für den vorliegenden Fall, dass selbst dann, wenn man die Klägerin, obwohl kein schriftlicher Auftrag vorliegt, allein deshalb als Auftraggeber ansehen wollte, weil sie mit der Einrichtung und dem Betrieb einer Fanpage Facebook in die Lage versetzt, personenbezogene Daten der Nutzer zu verarbeiten, dies wegen des ihr fehlenden Einflusses auf die Datenverarbeitung und der tatsächlich bestehenden alleinigen Herrschaft von Facebook über die Daten als verantwortliche Stelle ausscheidet. Aus diesem Grund hat der Beklagte in den Verfahren 4 MB 11/13 (a.a.O.) nicht einmal die Beigeladene als verantwortliche Stelle angesehen, obwohl die Beigeladene mit ihrer Konzernmutter, Facebook Inc. mit Sitz in den USA, vertraglich vereinbart hat, dass sie für die Verarbeitung von Daten von Facebook-Nutzern außerhalb Nordamerikas zuständig und verantwortlich ist, weil die rein rechtliche Zuweisung der Verantwortung an eine Stelle ohne entsprechende tatsächliche Übertragung der Einflussmöglichkeiten nicht ausreiche. Im vorliegenden Verfahren macht der Beklagte ebenfalls geltend, dass Facebook Inc. (USA) personenbezogene Daten in Deutschland verarbeite, und beruft sich auf die Entscheidung des Kammergerichts Berlin vom 24. Januar 2014 (a.a.O.). Danach soll eine eigene effektive und tatsächliche Datenverarbeitung durch die Beigeladene nicht erkennbar sein und eine Auftragsverarbeitung durch eine Muttergesellschaft für eine 100%ige Tochtergesellschaft nicht in Betracht kommen, weil die Konzernmutter Entscheidungsprozesse faktisch jeder Zeit an sich ziehen könne. Wenn danach selbst die Beigeladene keine verantwortliche

Stelle mangels hinreichenden Einflusses auf die Datenverarbeitung ist, ist schlechterdings nicht nachvollziehbar, weshalb die Klägerin, die weder Nutzerdaten erhebt noch irgendeinen Einfluss auf die Datenverarbeitung durch Facebook hat, verantwortliche Stelle sein könnte.

Die Ermächtigungsnorm des § 38 Abs. 5 BDSG erlaubt keine Anordnung gegenüber Dritten.

Dritter ist gemäß § 3 Abs. 8 S. 2 BDSG jede Person oder Stelle außerhalb der verantwortlichen Stelle.

Die von der zivilgerichtlichen Rechtsprechung entwickelte Störerhaftung im Internet, die Privaten Abwehransprüche zur Beseitigung erlittener Verletzung absoluter Rechte vermittelt (s. zum Urheberschutz BGH, Urt. v. 20.07.2010 - I ZR 139/08 -, K & R 2011, 117 u. Urt. v. 15.08.2013 - I ZR 80/12 -, NJW 2013, 3245), ist auf die Eingriffsverwaltung nicht übertragbar.

Die Ermächtigung gemäß § 38 Abs. 5 BDSG, Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel anzuordnen, muss den rechtsstaatlichen Anforderungen der Bestimmtheit und Klarheit einer gesetzlichen Ermächtigung genügen. Das Bestimmtheitsgebot soll sicherstellen, dass der demokratisch legitimierte Parlamentsgesetzgeber die wesentlichen Entscheidungen über Grundrechtseingriffe und deren Reichweite selbst trifft, dass Regierung und Verwaltung im Gesetz steuernde und begrenzende Handlungsmaßstäbe vorfinden und dass die Gerichte eine wirksame Rechtskontrolle ausführen können. Ferner erlauben die Bestimmtheit und Klarheit der Norm, dass der betroffene Bürger sich auf mögliche belastende Maßnahmen einstellen kann (s. hierzu zusammenfassend BVerfG, Urt. v. 11.03.2008 - 1 BvR 2074/05 u.a. -, BVerfGE 120, 378). Eine Eingriffsnorm, die nicht hinreichend deutlich erkennen lässt, welcher Personenkreis Adressat der Norm ist, genügt dem Bestimmtheitsgebot nicht. Ob dies der Fall ist, ist durch Auslegung zu ermitteln. Danach steht für den Senat außer Zweifel, dass Adressat der Anordnung des § 38 Abs. 5 BDSG nur eine verantwortliche Stelle im Sinne des § 3 Abs. 7 BDSG sein kann.

§ 38 Abs. 5 BDSG nennt den Adressaten der Anordnung nicht ausdrücklich. Allerdings gibt bereits der Wortlaut deutliche Hinweise. Nach § 38 Abs. 5 S. 1 BDSG dient die Anordnung der Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten oder tatsächlicher oder organisatorischer Mängel. Angesprochen ist damit die Datenverarbeitung als solche. Wie bereits ausgeführt, schreibt die Vorschrift ein abgestuftes Verfahren vor. Im ersten Schritt geht es darum, festgestellte Verstöße und Mängel der Datenverarbeitung konstruktiv zu beseitigen. Dies steht allein in der Macht des Datenverarbeiters. Erst dann, wenn die verantwortliche Stelle (so ausdrücklich Gola/Schomerus, a.a.O., § 38 Rn. 26) nicht wie nach Satz 1 angeordnet innerhalb der gesetzten Frist tätig wird und auch die Verhängung eines Zwangsgelds erfolglos bleibt, hat die Aufsichtsbehörde das Recht, den Einsatz eines „ungesicherten“ Verfahrens zu untersagen (ebenso Petri, a.a.O., § 38 Rn. 73).

§ 38 BDSG ist eine Vorschrift des dritten Abschnitts. Nach § 27 Abs. 1 BDSG finden die Vorschriften dieses Abschnitts Anwendung, soweit personenbezogene Daten unter anderem durch nicht-öffentliche Stellen verarbeitet, genutzt oder erhoben werden. Auch diese Vorschrift stellt auf die Datenverarbeitung als solche ab und begrenzt den Anwendungsbereich des § 38 Abs. 5 BDSG. Sie korrespondiert mit der Regelung des § 1 Abs. 2 BDSG über den Anwendungsbereich des Gesetzes, wonach das Gesetz für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch unter anderem nicht-öffentliche Stellen gilt (Abs. 2 Nr. 3). Der Begriff der nicht-öffentlichen Stellen wird in § 2 Abs. 4 BDSG definiert. In diesem Kontext ist auch die Begriffsbestimmung der verantwortlichen Stelle in § 3 Abs. 7 BDSG zu sehen, der als verantwortliche Stelle jede Person oder Stelle bezeichnet, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Letzteres ist keine Erweiterung, sondern lediglich eine Klarstellung, dass der Auftraggeber, der nicht selbst die Datenverarbeitung durchführt, sondern einen Verarbeiter einschaltet, verantwortliche Stelle ist (Dammann, a.a.O., § 3 Rn. 227 f). Der Begriff der verantwortlichen Stelle dient mithin als Anknüpfungspunkt für vom Gesetz festgelegte Rechte und Pflichten. Mit dem Begriff „Stelle“ verweist das Gesetz auf die Begriffsbestimmung des § 2 BDSG. Bezugspunkt der Verantwortlichkeit ist der Datenumgang (Dammann, a.a.O., § 3 Rn. 224). Knüpfen Rechte und Pflichten aus dem BDSG bei der verantwortlichen Stelle an, so bedeutet dies, dass sie tätig zu werden bzw. verbotene Handlungen (§ 4 BDSG) zu unterlassen hat und damit Normadressat ist (Dammann, a.a.O., § 3 Rn. 225). Eine Stelle, die keinen Einfluss auf die

Datenverarbeitung hat, ist weder verantwortlich noch kann von ihr verlangt werden, dass sie für die Einhaltung datenschutzrechtlicher Vorschriften Sorge trägt.

Dem steht nicht entgegen, dass § 11 Abs. 4 Nr. 2 BDSG für die übrigen nicht-öffentlichen Stellen (gemeint sind damit nicht-öffentliche Stellen, bei denen die öffentliche Hand nicht mehrheitsbeteiligt ist), die geschäftsmäßig im Auftrag als Dienstleistungsunternehmen personenbezogene Daten verarbeiten, § 38 BDSG gilt. Daraus lässt sich entgegen dem Vortrag des Beklagten nicht herleiten, dass Maßnahmen nicht allein an den Verantwortlichen gerichtet werden können. Die Auftragsverarbeiter sind Verantwortliche im Sinne des § 3 Abs. 7 BDSG. Ihre Verantwortlichkeit ist lediglich eingeschränkt (Dammann, a.a.O., § 3 Rn. 223). Was die Auftragsabwicklung anbelangt, gelten für den Auftragsverarbeiter diejenigen BDSG-Regelungen, die sich auf seinen Verantwortungsbereich beziehen (§ 11 Abs. 4 BDSG). Der Relativsatz in § 3 Abs. 7 BDSG, „die Daten für sich selbst erhebt“, kann nicht einschränkend dahingehend verstanden werden, dass der Auftragsverarbeiter deshalb keine verantwortliche Stelle im Sinne des § 3 Abs. 7 BDSG ist; dies würde zu der vom Gesetz in § 11 BDSG im Einzelnen geregelten Verantwortlichkeit im Widerspruch stehen (s. Dammann, a.a.O., § 3 Rn. 228). Die Richtlinie 95/46/EG unterscheidet allerdings begrifflich zwischen dem für die Verarbeitung Verantwortlichen (Art. 2 d)) und dem Auftragsverarbeiter (Art. 2 e)). Dies ändert aber nichts daran, dass der Auftragsverarbeiter eine Eigenverantwortung hat (Art. 17). Jedenfalls lässt sich aus der Vorschrift des § 11 Abs. 4 Nr. 2 BDSG nicht herleiten, dass darüber hinaus Dritte, die - im Gegensatz zum Auftragsverarbeiter - mit der Datenverarbeitung nicht befasst sind und auch keinerlei Einfluss darauf haben, wie Daten verarbeitet werden, gleichfalls Adressat einer Anordnung nach § 38 Abs. 5 BDSG sein können.

Die Auslegung, dass Anordnungen nach § 38 Abs. 5 BDSG nur gegenüber einer verantwortlichen Stelle ergehen können, wird auch durch die Gesetzeshistorie bestätigt. Vor Inkrafttreten des Gesetzes zur Änderung datenschutzrechtlicher Vorschriften am 1. September 2009 (BT-Dr. 16/13637) waren Anordnungs- und Untersagungsverfügungen auf die Beseitigung technischer und organisatorischer Mängel beschränkt. Die Änderung des § 38 Abs. 5 BDSG geht auf eine Initiative des Bundesrates (s. Anlage 3 zur BT-Dr. 16/12011 S. 44) zurück. Die Eingriffsbefugnisse der Aufsichtsbehörde in Bezug auf konkrete Datenverarbeitungen seien in § 38 Abs. 5 BDSG geregelt. Die Regelung erfasse materiell unzulässige Verarbeitungen und sonstige Verstöße gegen datenschutzrechtliche Vorschriften nicht. Deshalb sei es der Aufsichtsbehörde nicht möglich, ihre Rechtsauffas-

sung durchzusetzen. Für die Schaffung von Anordnungsbefugnissen für die Aufsichtsbehörden auch in Bezug auf materiell rechtswidrige Datenverarbeitung bzw. Verstöße gegen datenschutzrechtliche Vorschriften spreche Art. 28 Abs. 3, 2. Spiegelstrich der EG-Datenschutzrichtlinie, wonach die Kontrollstellen über wirksame Eingriffsbefugnisse verfügen müssten. Hierzu gehöre beispielsweise die Möglichkeit, das vorläufige oder endgültige Verbot einer Verarbeitung anzuordnen. Der Bundestag möge prüfen, ob die Eingriffsbefugnisse der Datenschutzbehörden dahingehend erweitert werden können, dass diese über § 38 Abs. 5 BDSG (alt) hinaus generell Anordnungen und Untersagungsverfügungen in Bezug auf materiell rechtswidrige Datenverarbeitung oder sonstige Verstöße gegen datenschutzrechtliche Vorschriften erlassen können. Dem Bundesrat ging es ersichtlich darum, die Eingriffsbefugnisse der Aufsichtsbehörde in Bezug auf konkrete Datenverarbeitungen zu erweitern und erstmals eine Eingriffsmöglichkeit bei materiell rechtswidrigen Verstößen gegen das Datenschutzrecht zu schaffen und dies mit Blick auf Art. 28 Abs. 3 RL 95/46/EG. Anhaltspunkte dafür, dass der Bundesrat die Befugnisse der Aufsichtsbehörde darüber hinaus im Hinblick auf Dritte erweitern wollte, die eine unzulässige Datenverarbeitung durch die nicht-öffentliche Stelle ermöglichen, ohne selbst verantwortliche Stelle im Sinne des § 3 Abs. 7 BDSG zu sein (Störer), sind dem Vorschlag nicht zu entnehmen. Der Bundestag ist dem Vorschlag mit der Neuregelung gemäß § 38 Abs. 5 BDSG gefolgt und hat das bereits beschriebene abgestufte Verfahren zur Beseitigung materiell rechtswidriger Datenverarbeitung eingeführt.

Eine Haftung nicht verantwortlicher Dritter, einschließlich eines Störers im Sinne des Gefahrenabwehrrechts, lässt sich aus der Richtlinie 95/46/EG nicht herleiten.

Die Richtlinie unterscheidet in Art. 2 zwischen „für die Verarbeitung Verantwortliche“ (a), „Auftragsverarbeiter“ (e) und „Dritter“ (f). Der Begriff „für die Verarbeitung Verantwortlicher“ und seine Wechselbeziehungen mit dem Begriff „Auftragsverarbeiter“ spielen eine wichtige Rolle bei der Anwendung der Richtlinie 95/46/EG, da sie bestimmen, wer für die Einhaltung der Datenschutzbestimmungen verantwortlich ist (Art. 29 - Datenschutzgruppe, WP 169 S. 1). Nach Art. 12 b) der Richtlinie garantieren die Mitgliedstaaten jeder betreffenden Person das Recht, vom für die Verarbeitung Verantwortlichen je nach Fall die Berichtigung, Löschung oder Sperrung von Daten, deren Verarbeitung nicht den Bestimmungen der Richtlinie entspricht ... zu erhalten. Nach Art. 23 Abs. 1 sehen die Mitgliedstaaten vor, dass jede Person, der wegen einer rechtswidrigen Verarbeitung oder jeder anderen mit den einzelstaatlichen Vorschriften zur Umsetzung dieser Richtlinie nicht zu

vereinbarenden Handlung ein Schaden entsteht, das Recht hat, von dem für die Verarbeitung Verantwortlichen Schadensersatz zu verlangen. Nach Art. 28 Abs. 3 - 2. Spiegelstrich - verfügt die Kontrollbehörde über wirksame Eingriffsbefugnisse, unter anderem über die Befugnis, die Sperrung, Löschung oder Vernichtung von Daten anzuordnen, was die betroffene Person nach Art. 12 b) von der verantwortlichen Stelle verlangen kann und auch nur der verantwortlichen Stelle möglich ist, gegebenenfalls durch Weisung an den Auftragsbearbeiter. Ausdrücklich wird die verantwortliche Stelle als Adressat einer Verwarnung oder Ermahnung genannt. Sie allein ist mithin die Adressatin einer niederschweligen Maßnahme, was der Annahme entgegensteht, dass schwerwiegende Eingriffe auch gegenüber Dritten möglich sein sollen. Eine Haftung eines Dritten, allein weil er einen Kausalbeitrag für die rechtswidrige Verarbeitung geleistet hat, der nicht die Qualität einer Datenverarbeitung erreicht und die Schwelle zur Einflussmöglichkeit auf die Datenverarbeitung nicht überschreitet, findet in der Richtlinie keine Grundlage (s. Piltz, K & R 2014, 80).

Schließlich ist dem Beklagten auch darin nicht zu folgen, dass ohne Rückgriff auf die allgemeinen Regelungen des Gefahrenabwehrrechts eine Schutzlücke bestehe.

Der Beklagte mag zwar Sonderordnungsbehörde im Sinne des § 164 Abs. 1 Nr. 4 LVwG sein, nach § 173 Abs. 2 LVwG gelten für die Durchführung der Gefahrenabwehr die §§ 174 bis 127 LVwG aber nur, soweit besondere Gesetze fehlen oder eine abschließende Regelung nicht enthalten. Die Regelung des § 38 Abs. 5 BDSG ist - aus den oben genannten Gründen - abschließend. Eine Schutzlücke besteht schon deshalb nicht, weil es für jede Datenverarbeitung eine verantwortliche Stelle gibt. Unverantwortliche Aktivitäten sind ausgeschlossen (Dammann, a.a.O., § 3 Rn. 224). Der Umstand, dass es womöglich umständlicher ist, gegenüber dem Verantwortlichen die Beseitigung von Datenverarbeitungs- und sonstigen Verstöße durchzusetzen, weil eine Zuständigkeit der Datenschutzbehörde, die den Verstoß festgestellt hat, nicht gegeben ist oder deutsches Datenschutzrecht nicht anwendbar ist, rechtfertigt die entsprechende Anwendung der Regelungen des Gefahrenabwehrrechts nicht. Eine planwidrige Lücke besteht nicht. Auch ist der Schutzpflicht aus Art. 8 EU-GrCH genügt, wenn die zuständige Kontrollbehörde gegen den für die Datenverarbeitung Verantwortlichen vorgehen kann.

Nach alledem bedarf es keiner Entscheidung, ob die Beklagte bzw. ihre Konzernmutter personenbezogene Daten verarbeitet und ob die Datenverarbeitung gegen deutsches bzw. irisches Datenschutzrecht verstößt. Allerdings steht für den Senat außer Frage, dass die Beigeladene jedenfalls dann personenbezogene Daten von Besuchern einer Fanpage verarbeitet, wenn es sich dabei um eingeloggte Facebook-Mitglieder handelt. Das folgt schon aus den Datenverwendungsrichtlinien von Facebook. Danach dienen die gesetzten Cookies dazu, Facebook-Nutzer zu erkennen und passende Inhalte für diese bereit zu stellen sowie Informationen über Facebook-Nutzer zu sammeln.

Die Kostenentscheidung folgt aus § 154 Abs. 2 VwGO, die Entscheidung über die vorläufige Vollstreckbarkeit beruht auf § 167 VwGO i.V.m. §§ 708 Nr. 10, 711 ZPO.

Die Revision ist zuzulassen, weil bisher nicht höchstrichterlich geklärt ist, ob Ausnahmen vom vorgeschriebenen abgestuften Verfahren des § 38 Abs. 5 BDSG möglich sind und gegebenenfalls, in welchen Fällen ausnahmsweise vom Wortlaut des § 38 Abs. 5 BDSG abgewichen werden kann, und ob eine Inanspruchnahme eines nicht im Sinne des § 3 Abs. 7 BDSG Verantwortlichen durch die Kontrollstelle als Störer datenschutzrechtlich in Betracht kommt.

Rechtsmittelbelehrung

Gegen dieses Urteil ist die Revision an das Bundesverwaltungsgericht statthaft. Die Revision ist bei dem

Schleswig-Holsteinischen
Oberverwaltungsgericht,
Brockdorff-Rantzau-Straße 13,
24837 Schleswig,

innerhalb eines Monats nach Zustellung des Urteils schriftlich einzulegen. Die Revisionsfrist ist auch gewahrt, wenn die Revision innerhalb der Frist bei dem Bundesverwaltungsgericht schriftlich oder in elektronischer Form nach Maßgabe der Verordnung über den elektronischen Rechtsverkehr beim Bundesverwaltungsgericht und beim Bundesfinanzhof vom 26.11.2004 (BGBl. I. S. 3091) eingelegt wird. Die Revisionsschrift muss das angefochtene Urteil bezeichnen.

Die Revision ist innerhalb von zwei Monaten nach der Zustellung des Urteils zu begründen. Die Begründung ist bei dem Bundesverwaltungsgericht oder in elektronischer Form nach Maßgabe der o. g. Verordnung vom 26.11.2004 einzureichen. Die Begründungsfrist kann auf einen vor ihrem Ablauf gestellten Antrag von dem Vorsitzenden des mit der Revision befassten Senats des Bundesverwaltungsgerichts verlängert werden.

Die Revisionsbegründung muss einen bestimmten Antrag enthalten, die verletzte Rechtsnorm und, soweit Verfahrensmängel gerügt werden, die Tatsachen angeben, die den Mangel ergeben. Im Revisionsverfahren müssen sich die Beteiligten durch Prozessbevollmächtigte vertreten lassen. Als Bevollmächtigte sind Rechtsanwälte und Rechtslehrer an einer deutschen Hochschule im Sinne des Hochschulrahmengesetzes mit Befähigung zum Richteramt zugelassen. Juristische Personen des öffentlichen Rechts und Behörden können sich auch durch Beamte oder Angestellte mit der Befähigung zum Richteramt oder Diplomjuristen im höheren Dienst vertreten lassen. Auf die weiteren Möglichkeiten der Prozessvertretung für Behörden und juristische Personen des öffentlichen Rechts einschließlich der von ihnen zur Erfüllung ihrer öffentlichen Aufgaben gebildeten Zusammenschlüsse wird hingewiesen (vgl. § 67 Abs. 4 S. 4 VwGO i. d. F. vom 12.12.2007 [BGBl. I. 2840] und § 5 Nr. 6 des Einführungsgesetzes zum Rechtsdienstleistungsgesetz i. d. F. vom 12.06.2008 [BGBl. I S. 1000]).

■■■■■■■■■■

■■■■■■■■■■

■■■■■■■■■■