ULD • Postfach 71 16 • 24171 Kiel

Schleswig-Holsteinisches Oberverwaltungsgericht
Brockdorff-Rantzau-Straße 13
24837 Schleswig

Vorab per Telefax: 04621/861277

Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223

Ansprechpartner/in:
Herr Dr. Polenz
Durchwahl: 988-1215

Aktenzeichen:
LD4-61.45/11.001

Kiel, 18. Dezember 2013

Verwaltungsrechtssache Unabhängiges Landeszentrum für Datenschutz ./. Wirtschaftsakademie Schleswig-Holstein GmbH
4 LB 20/13

Sehr geehrte Damen und Herren,

in vorbezeichneter Angelegenheit beantragen wir, das Urteil des Verwaltungsgerichts Schleswig vom 9. Oktober 2013, Az.: 8 A 14/12, abzuändern und die Klage abzuweisen.

Die Berufung begründen wir wie folgt:

A. Lückenhafte technische Bewertungsgrundlage

Das Verwaltungsgericht Schleswig erkennt die technischen Abläufe nur lückenhaft. Es erfasst dadurch nicht hinreichend, welche Bedeutung Fanpages für das Geschäftskonzept des „sozialen Netzwerkes" Facebook haben und welche Gefahren von den Fanpages für die Grundrechte der Bürger ausgehen.

Die Ursache der lückenhaften Bewertungsgrundlage mag darin liegen, dass das Verwaltungsgericht für die Darstellung der technischen Abläufe den Ergebnisbericht der Arbeitsgruppe des AK I „Staatsrecht und Verwaltung" zum Datenschutz in sozialen Netzwerken vom 04.04.2012 (VG Schleswig, Urteil vom 09.10.2013 – 8 A 14/12, S. 3 f.) nahezu im Wortlaut übernommen hat, ohne aber den Bericht der Arbeitsgruppe zur Fortentwicklung zu beachten (Bericht zur Fortentwicklungen des Sachstands seit dem Ergebnisbericht der Arbeitsgruppe des AK I zum Datenschutz in Sozialen Netzwerken vom 04.042012 mit Stand vom 31.07.2013, als **Anlage 1** diesem Schriftsatz beigefügt). Darin führt die Arbeitsgruppe aus (S. 5 des Berichts), dass Facebook neben den bekannten Cookies, wie dem c_user- und datr-Cookie, weitere Cookies verwendet, die Fragen aufwerfen:

> *„Im Zuge der Folgeuntersuchungen im Juli 2012 wurde darüber hinaus ein weiterer Cookie festgestellt, der beim Einloggen eines Facebook-Mitglieds auf der Seite gesetzt wird. Dieser sog. fr-Cookie hat eine Lebensdauer von 30 Tagen und enthält eine verschlüsselte Version der Nutzerkennung. Er wird nicht zu Sicherheitszwecken verwendet, sondern zur Unterstützung des Angebots relevanter Werbeanzeigen. Facebook wurde durch die irische Datenschutzaufsichtsbehörde aufgefordert, detaillierte Informationen über die Verwendung dieses Cookies und die hierfür eingeholte Einwilligung der Nutzer zu geben. Unabhängig vom Erfordernis einer Einwilligung für die Verwendung des Cookies als solchem (Art. 5 Abs. 3 der Richtlinie 2002/58/EG) erfordert der Einsatz des „fr-Cookies" als Speicherung und Nutzung personenbezogener Daten auch bei der Anwendung der Maßstäbe des deutschen Telemedienrechts eine Einwilligung der Facebook-Nutzer: Da für Facebook wegen der Möglichkeit der Zusammenführung von Nutzerprofilen und Stammdaten nicht nur ein pseudonymisiertes Nutzerprofil i.S.v. § 15 Abs. 3 TMG vorliegt, bedarf der Einsatz des Cookies einer eigenständigen datenschutzrechtlichen Rechtfertigung, zumal sein Einsatz auch nicht alleine – wie für den sog. datr-Cookie geltend gemacht wird – auf Sicherheitserfordernisse im Sinne von § 15 Abs. 1 TMG gestützt werden kann."*

Auch hat das Verwaltungsgericht nicht hinreichend die ergänzenden technischen Ausführungen des ULD zur datenschutzrechtlichen Bewertung der Reichweitenanalyse durch Facebook berücksichtigt (Anlage B 3 des Schriftsatzes des ULD vom 16.03.2012). Darin hat das ULD weitere Cookies aufgezeigt, die Facebook auf den informationstechnischen Systemen der Fanpagebesucher installiert. Nicht-authentifizierte Nutzer beispielsweise erhalten beim Aufruf der Webschnittstelle neben dem datr-Cookie, den Cookie „lsd", den Cookie „reg_fb_gate" und den Cookie „reg_fb_ref". Bei authentifizierten Nutzern werden neben den aufgeführten Cookies folgende Cookies gesetzt: Cookie „s", Cookie „sct", Cookie „xs" und Cookie „c_user". Diese Cookies dienen der Authentifizierung und sind einen Monat lang gültig. Meldet sich der Nutzer nicht aktiv ab, werden diese Cookies zumindest für einen Monat bei Aufruf der Webschnittstelle oder von Social-Plugins an Facebook übertragen.

Vor diesem Hintergrund betrachtet greift die Feststellung des Verwaltungsgericht zu kurz, dass die eingesetzten Cookies einzig der Identifizierung von Mitgliedern und dem Schutz des Netzwerkes vor „böswilligen Aktivitäten" dienen (VG Schleswig, Urteil vom 09.10.2013 – 8 A 14/12, S. 4). Einige dieser Cookies mögen zwar auch für diese Funktionen eingesetzt werden, wie es Facebook gerne vorgibt. Dabei verkennt das Verwaltungsgericht aber, dass allein schon aufgrund der Masse der verwendeten Cookies erhebliche Zweifel an dieser Behauptung von Facebook bestehen. Widerlegt wird diese letztlich dadurch, dass zahlreiche der Cookies erheblich länger auf den Systemen der Betroffenen gespeichert bleiben, als es für die Authentifizierung von Mitgliedern und die Funktionen und Sicherheit des Netzwerkes nötig ist. So bleibt beispielsweise der fr-Cookie einen Monat, der datr-Cookie sogar zwei Jahre auf den Systemen der Internetnutzer aktiv.

Das Gericht übersieht, dass die Cookies vielmehr eine zentrale Rolle für das Geschäftskonzept von Facebook spielen. Die Facebook.Inc ist ein weltweit tätiges, erfolgreiches, börsennotiertes Unternehmen, dass seinen Umsatz durch die Vermarktung adressatenbezogener zielgruppenorientierter Werbung generiert. Facebook selbst führt in seinen „Datenverwendungsrichtlinien" aus, dass es die vom Nutzer „bereit gestellten Informationen" nutzt, „um die Effektivität von Werbeanzeigen," die die Nutzer des Netzwerkes und andere Personen sehen, „zu messen und zu verstehen" (Anlage B 4 des Schriftsatzes des ULD vom 16.03.2012). Schließlich gibt Facebook in seinen Datenverwendungsrichtlinien gegenüber dem Nutzer an: „Durch die Angabe deines Geburtsdatums können wir dir altersan-

gemessene Inhalte und Werbeanzeigen anbieten“ (Anlage B 5 des Schriftsatzes des ULD vom 16.03.2012).

Insbesondere die langfristig gespeicherten Cookies (datr- und fr-Cookie) liefern für das lukrative Geschäftskonzept von Facebook die zentrale Infrastruktur. Solange Internetnutzer durch ihre Browsereinstellungen die Annahme von Cookies nicht verweigern oder diese löschen, bleiben die Cookies bis zu zwei Jahre auf den Computern, Smartphones oder Tablets der Besucher erhalten. Über diesen Zweitraum kann Facebook die markierten Systeme in breitem Umfang, weit über die eigene Plattform hinaus, wiedererkennen und das Verhalten der betroffenen Nutzer im Internet erfassen. Zahlreiche wichtige Webportalbetreiber integrieren nämlich mittlerweile in ihre eigenen Seiten „Social-Plug-Ins“ von Facebook. Ruft ein Internetnutzer etwa einen Nachrichtenartikel auf Spiegel-Online auf, wird durch den Plug-In automatisch in dessen Browser auch eine Facebook-Seite geladen, über die Facebook die Cookies des Seitenbesuchers ausliest. Dies geschieht letztlich unabhängig davon, ob der jeweilige Besucher gerade bei Facebook eingeloggt ist oder nicht. Auch ist unerheblich, ob der Internetnutzer überhaupt Mitglied bei Facebook ist. Hat er zuvor eine Fanpage aufgerufen, ist auch sein System in der Regel mit den Cookies gekennzeichnet. Auf diese Weise erhält Facebook umfangreiche Nutzungsdaten, aus denen es aussagekräftige Interessen und Persönlichkeitsprofile generiert und diese anschließend vermarktet.

Anders als es beim Verwaltungsgericht anklingt, sind die Fanpages deutlich mehr als ein „spezieller Benutzeraccount“ (VG Schleswig, Urteil vom 09.10.2013 – 8 A 14/12, S. 3).

Für Facebook sind Fanpagebetreiber, wie die Berufungsbeklagte, ein wichtiger Kooperationspartner, um Cookies zu verbreiten. Schließlich steigern die Fanpage-Angebote mit ihren Inhalten die Attraktivität des Netzwerkes für dessen Mitglieder. Vor allem aber locken die dort präsentierten Inhalte Internetnutzern auf die von Facebook bereit gestellte Infrastruktur, die bislang keine Facebook-Mitglieder sind. Bekannte Sportvereine, Musiker, Schauspieler und Unternehmen verbreiten Informationen zum Teil exklusiv über die Fanpages und erzeugen damit eine hohe Sogwirkung, die es immer schwerer macht, sich dem Tracking durch Facebook zu entziehen. Zudem bewerben die Fanpagebetreiber ihre Facebook-Angebote in Anzeigen und Werbespots. Die gängigen Suchmaschinen wie z. B. von Google weisen die Fanpages der Betreiber meist als hochrangige Treffer für die Suchworte der Betreiber in ihren Ergebnislisten aus. Dass die suchenden Internetnutzer dabei auf Facebook-Seiten gelangen, erkennen sie beim Anblick der Trefferlisten nur, soweit sie aufmerksam handeln und im Umgang mit dem Internet erfahren sind.

Aber auch die Fanpagebetreiber profitieren von der Fanpage und setzen diese ein, obwohl sie wissen, dass dadurch Profildaten der Nutzer zu Werbezwecken erhoben werden. Die Fanpage bietet ihnen eine leistungsstarke Infrastruktur für die Vermarktung von Inhalten im Internet. Sie zeichnet sich durch umfangreiche Serverkapazitäten, eine hohe Erreichbarkeit der Seiten und ein gutes Google-Ranking aus. Mit dem Einsatz der Fanpage spart die Berufungsbeklagte zudem weitere Kosten, die für vergleichbare herkömmliche Webhosting-Dienste entstehen würden, da sie diese Ressourcen kostenlos erhält. Auch an den im Rahmen des Netzwerkes erhobenen Nutzungsdaten partizipiert die Berufungsbeklagte als Fanpagebetreiber unmittelbar. Über die Funktion „Facebook-Insight“ werden ihr diese Daten in aggregierter Form aufbereitet, sodass sie aussagekräftige Statistiken über die Besucher ihrer Fanpage erhält und so die Wirksamkeit ihres Werbeauftritts in der Öffentlichkeit messen kann. Mit dem Betrieb der Fanpage nutzt die Berufungsbeklagte diese Vorteile und nimmt zugleich in Kauf, dass sie auf diese Weise weitere Besucher auf die von Facebook betriebene Infrastruktur lockt und damit einen wichtigen Beitrag leistet, damit deren Surfverhalten erfasst

wird. Des Weiteren wusste die Berufungsbeklagte beim Anlegen der Fanpage, dass sie bei diesem Angebot weniger Einfluss auf die Infrastruktur ausüben kann, als bei anderen Formen des Webhostings.

B. Verantwortlichkeit der Berufungsbeklagten für die Nutzungsdatenverarbeitung

In rechtlicher Hinsicht unterscheidet das Verwaltungsgericht zutreffend zwischen der Verantwortlichkeit für die Inhalte und der für die Nutzungsdaten. Nicht Gegenstand dieses Verfahren, aber unstreitig dürfte sein, dass die Betreiber von Facebook-Fanpages die datenschutzrechtliche Verantwortung für die von ihnen eingestellten Inhalte der Fanpages tragen (Weichert, Datenschutz bei Internetveröffentlichungen, VUR 2009, 323, 327).

Unzutreffend verneint das Verwaltungsgericht dagegen die Verantwortlichkeit der Fanpage-Betreiber für die mit der Nutzung der Fanpage durch die Besucher ausgelösten Verarbeitungsvorgänge.

I. Auftrag im Sinne von § 11 Abs. 2 BDSG

Das Gericht irrt, wenn es meint, dass die Verantwortlichkeit der Berufungsbeklagten als Auftragsdatenverarbeiter ausscheide, weil sie mit Facebook keinen wirksamen Auftrag im Sinne von § 11 Abs. 2 BDSG geschlossen habe (VG Schleswig, Urteil vom 09.10.2013 – 8 A 14/12, S. 17). Mit dieser Prüfung vermischt das Gericht in unzulässiger Weise Voraussetzungen und Rechtsfolge der Auftragsdatenverarbeitung. Der Vertrag im Sinne von § 11 Abs. 2 BDSG entscheidet nämlich nicht über die Verantwortlichkeit. Zusammen mit der Verantwortlichkeit der auslagernden Stelle ist der Auftrag nur eine von mehreren Voraussetzungen dafür, dass die Weitergabe der Daten an den Auftragsdatenverarbeiter privilegiert wird, indem sie ausnahmsweise keine Übermittlung darstellt (Jotzo, Der Schutz personenbezogener Daten in der Cloud, Baden-Baden 2013, S. 90 ff. Zur Privilegierung siehe Dammann, in: Kommentar zum BDSG, Simitis (Hrsg.), 7. Aufl. 2011, § 3 Rn. 244; Elbel, Zur Abgrenzung von Auftragsdatenverarbeitung und Übermittlung, RDV 2010, 203, 207). Das Vorliegen eines wirksamen Auftrages im Sinne von § 11 Abs. 2 BDSG taugt allenfalls als Indiz dafür, wie die beteiligten Stellen die Verantwortlichkeit untereinander verteilt haben (Art. 29 Datenschutzgruppe, WP 169, S. 33). Ob sie die Verantwortlichkeit tatsächlich auch so ausüben, ist allerdings eine andere Frage, die vorliegend die maßgebende ist (zum faktischen Ansatz der Verantwortlichkeit im Sinne der Richtlinie 95/46/EG: Art. 29 Datenschutzgruppe, WP 169, S. 10 ff.).

II. § 3 Abs. 7 BDSG in Verbindung mit Art. 2 d) RL 95/46/EG

Wann eine Stelle für die Einhaltung der Datenschutzvorschriften verantwortlich ist, regelt daher nicht § 11 BDSG, sondern allein die allgemeine Definition aus § 3 Abs. 7 BDSG.

Zutreffend nimmt das Verwaltungsgericht zwar an, dass § 3 Abs. 7 BDSG im Lichte von Art. 2 d) RL 95/46/EG ausgelegt werden muss (VG Schleswig, Urteil vom 09.10.2013 – 8 A 14/12, S. 16). Nach dieser Vorschrift ist für die Verarbeitung Verantwortlicher die natürliche oder juristische Person, Behör-

de, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Bei der Anwendung der Vorschrift verkennt das Gericht aber, dass die Berufsbeklagte als Fanpagebetreiber sowohl über Zweck als auch über die Mittel der Erhebung und Verarbeitung der Nutzungsdaten tatsächlich entscheidet. Das Gericht legt einen zu engen Maßstab an, wenn es die Verantwortung der Berufungsbeklagten verneint, weil diese mit „ihrem operativen Instrumentarium" in keinerlei direkten Kontakt zu dem Nutzer der Fanpage und dessen Daten komme (VG Schleswig, Urteil vom 09.10.2013 – 8 A 14/12, S. 17).

1.

a) Die Berufungsbeklagte entscheidet jedenfalls gemeinsam mit Facebook über den Zweck der Verarbeitung der Nutzungsdaten, indem sie ihre Fanpage angelegt hat und betreibt (Spindler, Persönlichkeitsschutz im Internet – Anforderungen und Grenzen einer Regulierung, Gutachten F zum 69. Deutschen Juristentag, 2012, F 81 f.; zu „Social Plug-Ins" so auch Ernst, Social Plugins: Der „Like-Button" als datenschutzrechtliches Problem, NJOZ 2010, 1917, 1918).

Sie weiß nämlich, dass Facebook Nutzungsdaten mit Hilfe von Cookies über die Besucher der Fanpages erzeugt, um Nutzerstatistiken zu erstellen. Diese Verarbeitungsvorgänge erfolgen auch im Interesse der Berufungsbeklagten, da sie über die Funktion „Facebook Insights" umfangreiche Informationen über die Besucher ihrer Fanpage erhält, mit denen sie den Erfolg ihres Webauftrittes beurteilt. Diese Funktion ist integraler Bestandteil der von ihr eingerichteten Fanpage und unterscheidet die Fanpage von anderen Webhosting-Angeboten. Dem entsprechen die Ausführungen der Berufungsbeklagten aus ihrem Schriftsatz vom 19. Januar 2012 (S. 2). Demnach betreibe die Berufungsbeklagte die Fanpage „insbesondere zu werblichen Zwecken für die eigenen Angebote, wie beispielsweise zur Ankündigung von aktuellen Veranstaltungen". Sie nutze die Fanpage in diesem Zusammenhang für Werbezwecke und zur bedarfsgerechten Gestaltung der angebotenen Telemedien.

b) Ob allein die vorliegende Entscheidung über den Zweck bereits die datenschutzrechtliche Verantwortlichkeit der Berufungsbeklagten bedingt (so allgemein die Art. 29 Datenschutzgruppe, WP 169, S. 17) kann dahinstehen, da die Berufungsbeklagte vorliegend auch über die Mittel der Datenverarbeitung im Sinne der Richtlinie entscheidet.

Anders als das Verwaltungsgericht meint, steht dem nicht entgegen, dass die Berufungsbeklagte nicht unmittelbar auf die erhobenen Nutzungsdaten und die technischen Abläufe zugreifen kann. Die für die einheitliche Anwendung der Richtlinie in den Mitgliedsstaaten berufene Art. 29 Datenschutzgruppe (Art. 30 Abs. 1 a) RL 95/46/EG) hat hierzu nämlich ausgeführt, dass die Entscheidung über die „Mittel" nicht die technischen Abläufe beinhalten müsse, 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 festlegt (Art. 29 Datenschutzgruppe, WP 169, S. 17). Diese Anforderungen erfüllt die Berufungsbeklagte, da sie bewusst die Fanpage mit der darin enthaltenen „Insights"-Funktion einsetzt. Zudem leisten die Fanpagebetreiber durch das Einstellen von Inhalten einen wesentlichen Beitrag für die Erhebung und Verarbeitung der Nutzungsdaten. Sie versorgen die Facebook-Infrastruktur mit Inhalten, füllen damit die Infrastruktur mit Leben und ziehen so die Betroffenen auf die Seiten von Facebook. Diese Tätigkeit der Fanpagebetreiber spielt eine Schlüsselrolle im Gesamt-

konzept der Fanpage und damit auch der Nutzungsdatenverarbeitung. Insoweit besteht ein Abhängigkeitsverhältnis zwischen Facebook und der Berufungsbeklagten.

2. Im Gegensatz zum Verwaltungsgericht schafft die Art. 29 Datenschutzgruppe mit ihrer Auslegung von Art. 2 d) RL 95/46/EG den nötigen Freiraum, um den besonderen Bedürfnissen bei der Auftragsdatenverarbeitung gerecht zu werden (zu den Interessen bei der Auftragsdatenverarbeitung Kramer/Herrmann, Auftragsdatenverarbeitung, CR 2003, 938, 939). Wer hier konkrete technische Vorgaben der auslagernden – aber verantwortlichen – Stelle für die vom Auftragsdatenverarbeiter ausgeführten Vorgänge fordert, nimmt datenverarbeitenden Stellen die Möglichkeit, Daten durch externe Anbieter verarbeiten zu lassen, um Vorgänge effizienter und kostensparender zu gestalten (Sutschet, Auftragsdatenverarbeitung und Funktionsübertragung, RDV 2004, 97, 101).

Anders als das Verwaltungsgericht verliert die Art. 29 Datenschutzgruppe mit ihrem Verständnis vor allem aber nicht den Zweck der Verantwortlichkeit aus den Augen. Art. 2 d) RL 95/46/EG soll für den Betroffenen und die Aufsichtsbehörden transparent festlegen, wer als Normadressat dafür einstehen muss, dass die Datenschutzregeln eingehalten werden (Art. 29 Datenschutzgruppe, WP 169, S. 6; Sutschet, Auftragsdatenverarbeitung und Funktionsübertragung, RDV 2004, 97, 100). Für die Betroffenen und die Behörden muss erkennbar sein, wer verantwortlich ist, da die Betroffenen andernfalls nicht ihre durch Art. 8 Abs. 2 Charta der Grundrechte der Europäischen Union (Eu-GrCh) und Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verbürgten Rechte effektiv durchsetzen und die Aufsichtsbehörden nicht die Einhaltung der Regeln überwachen könnten (Zum Konkurrenzverhältnis der europäischen und nationalen Grundrechte beim Schutz personenbezogener Daten: Masing, Herausforderungen des Datenschutzes, NJW 2012, 2305 ff.).

Zu dieser Auslegung zwingt das Gebot effektiven Grundrechtsschutzes, aus dem eine staatliche Schutzpflicht folgt, die auch für das Recht auf informationelle Selbstbestimmung besteht (Rupp, Die grundrechtliche Schutzpflicht des Staates für das Recht auf informationelle Selbstbestimmung im Pressesektor, 2013, S. 106 ff.; Hoffmann-Riem, AöR 123 (1998), 524). Sie gebietet den zuständigen staatlichen Stellen, die rechtlichen Voraussetzungen eines wirkungsvollen informationellen Selbstschutzes bereitzustellen (Ständige Rechtsprechung, siehe nur BVerfG NJW 2013, 3086 Tz. 21 – Datenschutz im privaten Versicherungsrecht; MMR 2007, 93 – Schweigepflichtentbindung). Diese Schutzpflicht gewinnt gerade bei den immer arbeitsteiliger werdenden Verarbeitungsprozessen im Internet stark an Bedeutung. Sie gewährleistet, dass der Bürger auch angesichts neuer Gefährdungen seine Grundrechte effektiv durchsetzen kann. Für den Grundrechtsschutz im digitalen Umfeld ist diese Schutzpflicht mittlerweile elementar, da der Gesetzgeber auf den dort stattfindenden rasanten Fortschritt nur verzögert reagieren kann.

3. Das Verwaltungsgericht berücksichtigt diese grundrechtlichen Vorgaben bei seiner Auslegung von § 3 Abs. 7 BDSG und Art. 2 d) RL 95/46/EG nicht ausreichend:

Dem Betroffenen mag zwar bewusst sein, dass er sich auf einer Facebook-Seite befindet. Aufgesucht hat er die Seite aber allein, um die Inhalte zu konsumieren, die der Fanpagebetreiber dort eingestellt hat. Welche technischen und rechtlichen Einflussmöglichkeiten der Inhalte-Anbieter auf die von ihm eingesetzte Infrastruktur hat, kann der Besucher in Zeiten des weltweiten vernetzten Rechnens aber weder erkennen, noch möchte er dies. Vielmehr vertraut er darauf, dass er seine Rechte gegenüber dem Anbieter der Inhalte durchsetzen kann, da dieser es in der Hand hat, vertrauenswürdige Dienstleister für die von ihm benötigte Infrastruktur zu wählen.

Dieser Linie folgend hat die Art. 29 Datenschutzgruppe auch die Anbieter von Online-Inhalten zusammen mit den Betreibern von Werbenetzen als gemeinsame Verantwortliche für die Verarbeitung von Nutzungsdaten von Besuchern ihrer Webseiten mittels Cookie eingestuft. Als Anknüpfungspunkt für die dazu erforderliche Entscheidung über die Mittel der Datenverarbeitung hat die Art. 29 Datenschutzgruppe angesehen, dass die Anbieter der Inhalte ihre Webseiten so konfiguriert haben, dass die Werbeanzeigen automatisch eingeblendet und die Besucher so auf die Webseiten der Betreiber der Werbenetze umgeleitet wurden (Art. 29 Datenschutzgruppe, WP 171, S. 13 ff.). Das Verwaltungsgericht nimmt irrtümlich an, dass dieser erste erforderliche Schritt zur Ermöglichung der Verarbeitungsvorgänge durch den Werbedienstleister im vorliegenden Fall gerade fehle. Diese Einschätzung geht fehl, da die Berufungsbeklagte bewusst die Infrastruktur von Facebook gewählt hat, um ihre Inhalte im Netz zu präsentieren und um sich zu vermarkten. Ebenso wie bei der Einbindung von Tracking-Tools, ermöglicht sie auf diese Weise, dass ein externer Anbieter die Daten ihrer Webseitenbesucher zu Werbezwecken mittels Cookies erfasst.

Dem Transparenzgedanken hat der Gesetzgeber auch an anderer Stelle im Medienrecht Rechnung getragen. Es entspricht dem Zweck der Impressumspflicht aus § 5 TMG, dass datenschutzrechtlich verantwortlich ist, wer aus Sicht des Nutzers für den Betrieb der Webseite als verantwortliche Stelle erscheint. Mit der Pflicht zur Angabe von Identität und Anschrift des Dienstanbieters soll diese Vorschrift die Rechtsverfolgung gewährleisten (BT-Drs. 13/7385, S. 21). § 5 TMG zielt auch darauf ab, dass der Nutzer gegenüber dem Anbieter seinen datenschutzrechtlichen Auskunftsanspruch nach § 13 Abs. 7 TMG, § 34 Abs. 1 BDSG geltend machen kann (vgl. Micklitz, in: Spindler/Schuster, Recht der elektronischen Medien, 2008, § 5 TMG, Rn. 4; Woitke, NJW 2003, 871, Das „Wie" der Anbieterkennzeichnung nach § 6 TDG; Bizer/Trosch, DuD 1999, 621). Hier auf die für den Nutzer verborgenden technischen Abläufe abzustellen widerspräche dem.

4. Bei der Auslegung der Verantwortlichkeit ist zudem zu berücksichtigen, dass diese Regelung sowohl für den öffentlichen wie auch den nichtöffentlichen Bereich gilt und einheitlich angewendet werden muss. Folgte man der Auslegung des VG Schleswig, so könnten sich nicht nur private, sondern auch öffentliche, einer besonderen Grundrechtsbindung unterliegenden Stellen ihrer datenschutzrechtlichen Verantwortung entziehen, indem sie Internetseiten nicht eigenverantwortlich betreiben, sondern deren Betrieb auf Dritte übertragen, die dann ausschließlich verantwortlich wären und faktisch nicht oder nur sehr schwer zur Verantwortung gezogen werden könnten. Welche Konsequenzen sich hieraus ergäben, zeigt sich beim Betrieb von Fanpages bei Facebook etwa durch Schulen oder Polizeidienststellen, über die von diesen Stellen Internetverkehr veranlasst wird, der letztlich ausschließlich tatsächlich und technisch von Facebook kontrolliert werden kann. Betroffen wären oft Minderjährige sowie Menschen, die sich in einer Notlage an eine öffentliche Stelle wenden (wollen). Mit der Interpretation des VG Schleswig würde auch den öffentlichen Stellen ein Weg eröffnet, sich ihrer Grundrechtsverantwortung im Hinblick auf die informationelle Selbstbestimmung gegenüber den Bürgerinnen und Bürgern zu entziehen.

5. Die vom Verwaltungsgericht vertretene Ansicht führt im Übrigen zu erheblichen Schutzlücken. Sollte der datenschutzrechtlichen Verantwortlichkeit bereits entgegenstehen, dass die verantwortliche Stelle keinen technischen Einfluss auf die Verarbeitungsprozesse ihres Infrastruktur-Anbieters hat, müssten Dienstanbieter einzig ihre eigene Anwendung kontrollieren. Was der von ihnen eingesetzte Infrastrukturanbieter dagegen mit den Daten ihrer Nutzer macht, müsste sie selbst dann nicht stören, wenn sie dessen rechtwidrige Handlungen kennen.

C. Störerhaftung der Wirtschaftsakademie Schleswig-Holstein GmbH

Sollte das Gericht wider Erwartung die Verantwortlichkeit der Berufungsbeklagten für die Nutzungsdatenvorgänge ablehnen, müssen die aufgezeigten Schutzdefizite jedenfalls durch die Anwendung der Grundsätze der Störerhaftung geschlossen werden. Das Gebot eines effektiven Grundrechtsschutzes verlangt, dass Betroffene und Aufsichtsbehörden Möglichkeiten haben, um gegen diejenigen Inhalte-Anbieter vorzugehenden, die für ihre Dienste wissentlich datenschutzrechtswidrige Infrastrukturbetreiber einsetzen.

Das Verwaltungsgericht Schleswig hat den dazu nötigen Rückgriff auf die allgemeinen Zurechnungsnormen aus dem Polizei- und Ordnungsrecht fälscherweise verneint (Urteil vom 09.10.2013 – 8 A 14/12, S. 19) und damit die ihm aus Art. 8 Eu-GrCh beziehungsweise Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG obliegende staatliche Schutzpflicht für das Recht auf informationelle Selbstbestimmung (BVerfG, NJW 2013, 3086 Tz. 21 – Datenschutz im privaten Versicherungsrecht; MMR 2007, 93 – Schweigepflichtentbindung) verletzt.

I. Keine abschließende Regelung der Inanspruchnahme durch die allgemeine Datenschutzrichtlinie

Anders als das Verwaltungsgericht meint (Urteil vom 09.10.2013 – 8 A 14/12, S. 20) steht dem insbesondere Art. 2 d) RL 95/46/EG nicht entgegen (Für die Anwendbarkeit der Störerhaftung im Datenschutzrecht: Piltz, Der Like-Button von Facebook, CR 2011, 657, 662 f.; Spindler, Datenschutz- und Persönlichkeitsrechte im Internet – der Rahmen für Forschungsaufgaben und Reformbedarf, GRUR 2013, 996, 1003. Dagegen: Voigt/Alich, Facebook-Like-Button und Co. – Datenschutzrechtliche Verantwortlichkeit der Webseitenbetreiber, NJW 2011, 3541, 3543).

1. Nichts anderes folgt aus den vom Gericht zitierten Entscheidungen des EuGH in den Rechtssachen C-468/10 und C-469/10, da diese den Harmonisierungsgrad der Richtlinie für die in Kapitel II der Richtlinie geregelten Erlaubnisgründe betreffen (EuGH, Urteil vom 24.11.2011, verb. Rs. C-468/10 und C-469/10, Tz. 24 ff. – ASNEF/FECEMD). Daraus kann aber nicht ohne Weiteres auf den vollharmonisierenden oder gar abschließenden Charakter der Richtlinie im Ganzen geschlossen werden. Schließlich muss für jeden Regelungsbereich einer Richtlinie ermittelt werden, welchen Umsetzungsraum deren Wortlaut, Zweck und System den Mitgliedsstaaten belässt (EuGH, Urteil vom 25.04.2004, Rs. C-183/00, Tz 25).

2. Gemessen an diesen Grundsätzen erkennt das Verwaltungsgericht zwar zutreffend, dass die Richtlinie den Begriff des „für die Verarbeitung Verantwortlichen“ vollharmonisierend regelt.

Weder der Wortlaut, noch der Zweck und das System der Richtlinie fordern aber, dass die Richtlinie auch abschließend festlegt, wer bei Datenschutzverstößen in Anspruch genommen werden kann.

Mit dem Konzept der Verantwortlichkeit hat der europäische Gesetzgeber nämlich einzig – und insoweit abschließend – vorgegeben, wer die aus dem Datenschutzrecht folgenden Pflichten erfüllen muss. Im Gegensatz dazu sieht die Störerhaftung keine positiven Handlungspflichten vor. Sie liefert einzig negative Unterlassungsansprüche gegen denjenigen, der durch kausale Beiträge Rechtsverletzungen fördert, die andere begehen. Da der Störer gerade kein Beteiligter der (Datenschutz-)Verstöße ist, fällt die Störerhaftung also nicht in den Anwendungsbereich der Richtlinie.

Zudem ist die Störerhaftung Teil der allgemeinen nationalen Haftungsgrundsätze, die von den europäischen Regeln unberührt bleiben. Insoweit würde es dem europäischen Gesetzgeber im Übrigen an der erforderlichen Kompetenz fehlen. Dieser Sicht folgt auch die Art. 29 Datenschutzgruppe. In ihrer zentralen Stellungnahme zur datenschutzrechtlichen Verantwortlichkeit stellt die Gruppe fest, dass die Richtlinie nicht ausschließe, dass „nationale Rechtsvorschriften eine Haftung nicht nur für den für die Verarbeitung Verantwortlichen vorsehen, sondern auch für jede andere Person, die gegen das Datenschutzrecht verstößt“ (WP 169, S. 20, Fn. 15).

Auch der Zweck der Richtlinie zwingt dazu, dass neben der datenschutzrechtlichen Verantwortlichkeit Raum für die allgemeinen Grundsätze der Störerhaftung bleibt. Art. 1 Abs. 1 RL 95/46/EG verpflichtet nämlich die Mitgliedstaaten, den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten zu gewährleisten. Diese Zweckbestimmung wird weiter ausgefüllt durch die primärrechtlichen Vorgaben aus Art. 8 EU-GrCh, in dessen Licht die Richtlinie ausgelegt werden muss (Art. 51 Abs. 1 EU-GrCh). Wie bereits gezeigt, führen die vom Verwaltungsgericht Schleswig vertretenen hohen Anforderungen an die Verantwortlichkeit aber zu Schutzlücken, die dem Zweck der Richtlinie nicht mehr gerecht werden. Nach den Maßstäben des Gerichts könnten Betroffene und Aufsichtsbehörden die Anbieter von Inhalten selbst dann nicht datenschutzrechtlich auf Unterlassung in Anspruch nehmen, wenn diese bewusst für ihre Internetdienste Infrastrukturbetreiber einsetzen, die datenschutzrechtswidrig handeln. Gerade in Zeiten des Cloud-Computings und den immer arbeitsteiliger werdenden Verarbeitungsstrukturen im digitalen Raum, würde diese Sicht eine Gefährdungslage schaffen, die das Grundrecht auf Schutz personenbezogener Daten im Kern bedroht.

3. Vor diesem Hintergrund betrachtet verwundert es nicht, dass auch der BGH in seiner Entscheidung zur datenschutzrechtlichen Zulässigkeit von Lehrerbewertungen im Internet die Grundsätze der Störerhaftung angewandt hat, ohne auch nur die vom Verwaltungsgericht aufgeworfene Frage anzusprechen (BGH, NJW 2009, 2888 ff. - spickmich). Den gegen den Portalbetreiber gerichteten Unterlassungsanspruch versagte das Gericht zwar, weil die Richter die Verarbeitungsvorgänge als gerechtfertigt einstuften (§ 29 BDSG). Unabhängig davon führten sie aber aus, dass die Betreiberin des Bewertungsportals als verantwortliche Mitstörerin in Betracht komme, weil sie mögliche Beeinträchtigungen Dritter zumindest mittelbar zu verantworten habe (BGH, NJW 2009, 2888, 2890).

4. Auch das BDSG gibt den für die Auslegung nötigen Raum, damit die Aufsichtsbehörden Anordnungen gegen den Störer treffen können. Aus dem Wortlaut von § 38 Abs. 5 BDSG folgt jedenfalls nicht, dass die Behörde die Anordnung ausschließlich gegenüber verantwortlichen Stellen aussprechen dürfen. Zur Gewährleistung der Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz kann die Behörde nach § 38 Abs. 5 BDSG vielmehr Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel anordnen. Bei schwerwiegenden Verstößen oder Mängeln, insbesondere solchen, die mit einer besonderen Gefährdung des Persönlichkeitsrechts verbunden sind, kann sie die Erhebung, Verarbeitung oder Nutzung oder den Einsatz einzelner Verfahren untersagen, wenn die Verstöße oder Mängel entgegen der Anordnung nach Satz 1 und trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden. § 38 Abs. 5 BDSG benennt ausdrücklich keinen bestimmten Adressaten. Aus dem Gesetzeszusammenhang ergibt sich zwar, dass Adressat der Maßnahmen die verantwortliche Stelle sein kann. Allein § 11 Abs. 4 Nr. 2 BDSG zeigt aber, dass die Maßnahmen nicht allein an den Verantwortlichen, sondern auch an andere Stellen gerichtet werden können, wie etwa Auftragsdatenverarbeiter.

II. Voraussetzungen der Inanspruchnahme der Berufungsbeklagten als Zweckveranlasser

Der Berufungskläger hat vorliegend auch zutreffend die Berufungsbeklagte mit Bescheid vom 3. November 2011 als Zweckveranlasser in Anspruch genommen.

1. Rechtsfigur des Zweckveranlassers

Die Rechtsfigur des Zweckveranlassers ist als besondere Form des Handlungsstörers anerkannt und wird von der Rechtsprechung in zahlreichen Bereichen des besonderen Verwaltungsrechts nutzbar gemacht (im Überblick Schoch, in: Schmidt-Aßmann/Schoch (Hrsg.), Verwaltungsrecht Besonderer Teil, 14. Aufl. 2008, 2. Kap. 138). So beispielweise im Polizei- und Ordnungsrecht, dem Sonn- und Feiertagsrecht, im Gaststättenrecht oder im Umweltrecht (vgl. etwa OVG Schleswig, Urteil vom 31.1.2002 – 4 L 107/01, juris-Tz. 43; VG Minden, NVwZ 1988, 638, 639; OVG Hamburg, NVwZ 1991, 180, 183; OVG Saarland, NVwZ 1993, 201; VGH Mannheim, NVwZ-RR 1995, 663; NdsOVG, NVwZ 1997, 622). Dahinter steht der allgemeine Rechtsgrundsatz, dass eine ordnungsbehördliche Heranziehung derjenigen Personen möglich sein muss, die durch ihre neutralen Handlungen Dritte dazu veranlassen, die öffentliche Sicherheit beziehungsweise Ordnung zu gefährden oder gar zu stören.

2. Anwendung des Zweckveranlassers im Datenschutzrecht

Entgegen den Ausführungen des VG Schleswig finden die §§ 173 ff. LVwG-SH und damit auch die Figur des Zweckveranlassers als Unterfall des Verhaltensverantwortlichen auch im Datenschutzrecht Anwendung.

Gemäß § 173 Abs. 1 LVwG führen Polizei- und Ordnungsbehörden wie das ULD zwar die Aufgabe der Gefahrenabwehr nach den besonderen Regelungen ihres jeweiligen Ordnungsrechts durch. Soweit diese aber fehlen oder eine abschließende Regelung nicht enthalten, gelten die allgemeinen Regeln des Gefahrenabwehrrechts aus den §§ 174 bis 227 LVwG-SH, § 173 Abs. 2 LVwG-SH. Das ist hier der Fall, da Landes- und Bundesdatenschutzgesetz einzig die positiven Handlungspflichten der verantwortlichen Stelle regeln, nicht aber die Inanspruchnahme weiterer Stellen als Störer. Das BDSG enthält insoweit auch keine abschließende Regelung. Dies zeigt bereits der offene Wortlaut von § 38 Abs. 5, der gerade keinen Adressaten der Anordnung nennt und damit Raum für die Inanspruchnahme weiterer Stellen neben dem datenschutzrechtlich Verantwortlichen lässt (C.I.4.). Gegen die abschließende Regelung des BDSG spricht zudem, dass ohne die Störerhaftung das Recht auf informationelle Selbstbestimmung der Betroffenen nicht hinreichend geschützt werden könnte. Hinsichtlich der deshalb greifenden staatlichen Schutzpflicht gelten die Einzelheiten, die bereits zum Verhältnis von datenschutzrechtlicher Verantwortlichkeit im Sinne der Datenschutzrichtlinie zur Störerhaftung gezeigt worden sind und auf die verwiesen wird (C.I.2.).

3. Materielle Rechtmäßigkeit der Inanspruchnahme

Die Berufungsbeklagte erfüllt mit ihrem Verhalten auch die Voraussetzungen für die Inanspruchnahme als Zweckveranlasser. Eine Zweckveranlassung besteht, wenn nach einer wertenden Betrach-

tung, zwischen der Gefahr und dem Verhalten desjenigen, der hierfür zwar nicht die letzte Ursache gesetzt, aber dennoch einen kausalen Beitrag geleistet hat, ein derartiger Wirkungs- und Verantwortungszusammenhang besteht, dass eine Zurechnung gerechtfertigt erscheint. Handlung und Erfolg müssen eine natürliche Einheit bilden (OVG Schleswig, Urteil vom 31.01.2002 – 4 L 107/01, juris-Tz. 43; VG Schleswig, NVwZ 2000, 464, 465).

Diese Voraussetzungen liegen hier vor, da Facebook datenschutzrechtswidrig Nutzungsdaten verarbeitet (aa) und die Berufungsbeklagte mit dem Betrieb der Fanpage einen Beitrag leistet, der mit der Störung eine natürliche Handlungseinheit bildet (bb).

aa) Datenschutzrechtswidrige Verarbeitung durch Facebook

Mit dem Dienst Facebook-Insights verstößt Facebook gegen geltendes Datenschutzrecht. Dabei kann dahinstehen, ob die Handlungen des Netzwerkbetreibers nach § 1 Abs. 5 Satz 2 BDSG dem deutschen oder gemäß § 1 Abs. 5 Satz 1 BDSG dem irischen Datenschutzrecht unterliegen (für die Anwendung des irischen Rechts: OVG Schleswig, NJW 2013, 1977 ff., in einem Verfahren des Eilrechtsschutzes), da die Nutzungsdatenerhebung zu Werbezwecken sowohl gegen deutsches (§ 15 Abs. 3 Satz 2 TMG), als auch gegen irisches Datenschutzrecht verstößt. Für das irische Recht folgt dies aus dem Data Protection Act 1988 (Number 25 of 1988) i.V.m. den Anpassungen aus dem Jahre 2003, dem Data Protection (Amendment) Act 2003 (Number 6 of 2003). Dessen Section 2A (1) sieht eine mit dem Erlaubnisvorbehalt aus § 4 Abs. 1 BDSG vergleichbare Regelung vor:

> *Processing of personal data.*
>
> *2A. (1) Personal data shall not be processed by a data controller unless section 2 of this Act (as amended by the Act of 2003) is complied with by the data controller and at least one of the following conditions is met:"*

Für den Dienst „Facebook-Insights" erhebt, verarbeitet und nutzt Facebook mittels Cookies Daten der Besucher von Facebook-Fanpages für Marketing- und Werbezwecke, ohne dass die nach Sec. 2A (1) Data Protection (Amendment) Act 2003 erforderliche Erlaubnis vorliegt.

(1) Als Erlaubnisnorm scheidet für die Datenverarbeitungsprozesse von „Facebook-Insights" insbesondere die Einwilligung der Betroffenen aus. Diese sieht das irische Datenschutzrecht zwar in Sec. 2A (1) (a) Data Protection (Amendment) Act 2003 vor:

> *(a) the data subject has given his or her consent to the processing or, if the data subject, by reason of his or her physical or mental incapacity or age, is or is likely to be unable to appreciate the nature and effect of such consent, it is given by a parent or guardian or a grandparent, uncle, aunt, brother or sister of the data subject and the giving of such consent is not prohibited by law,"*

Sec. 2A (1) (a) Data Protection (Amendment) Act 2003 rechtfertigt indes nicht die Verarbeitungsprozesse für „Facebook-Insights", da deren Voraussetzungen nicht erfüllt sind:

Auch die näheren Wirksamkeitsvoraussetzungen der Einwilligung nach Sec. 2A (1) (a) Data Protection (Amendment) Act 2003 folgen aus den europäischen Vorgaben. Nach Art. 5 RL 95/46/EG können die Mitgliedsstaaten zwar näher die Voraussetzungen bestimmen, unter denen die Verarbeitung

personenbezogener Daten rechtmäßig ist. Dabei müssen die Mitgliedsstaaten aber „nach Maßgabe" der in Kapitel II der Richtlinie geregelten Voraussetzungen handeln. Daher dürfen sie weder eigene Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung personenbezogener Daten neben Art. 7 der Richtlinie einführen, noch zusätzliche Bedingungen stellen, die die Tragweite eines der sechs in diesem Artikel vorgesehenen Grundsätze verändern würden (EuGH, Urteil vom 24.11.2011, verb. Rs. C-468/10 und C-469/10, Tz. 32 – ASNEF/FECEMD). Selbst im Bereich der Erlaubnisgründe lässt die Richtlinie den Mitgliedsstaaten daher nur einen bescheidenen Umsetzungsspielraum (Jotzo, Der Schutz personenbezogener Daten in der Cloud, Baden-Baden 2013, S. 36).

Gemäß der allgemeinen Begriffsbestimmung in Art. 2 h) RL 95/46/EG setzt die Einwilligung des Betroffenen voraus, dass dieser „in Kenntnis der Sachlage" im konkreten Fall die Datenverarbeitung akzeptiert. Damit der Betroffene eine solche Einwilligung abgeben kann, muss der Verantwortliche ihn insbesondere über die in Art. 10 RL 95/46/EG genannten Punkte informieren (Art. 29 Datenschutzgruppe, WP 187, S. 23). Hierzu zählen insbesondere die Identität der verantwortlichen Stelle (Art. 10 a) RL 95/46/EG) und die Zweckbestimmung der Verarbeitung (Art. 10 a) RL 95/46/EG). Diese Information sollen den betroffenen Personen die Gelegenheit bieten zu prüfen, ob die erbetenen Daten den genannten Zwecken entsprechen und rechtmäßig erhoben werden können (Dammann/Simitis, Kommentar zur EG-Datenschutzrichtlinie, 1997, Art. 10, Erl. 8 und Art. 2, Erl. 24). Informiert der Verantwortliche den Betroffenen unrichtig oder unvollständig, ist die Einwilligung unwirksam (Dammann/Simitis, aaO., Art. 2, Rz. 24).

Facebook erfüllt diese Anforderungen aus Art. 2 h) i.V.m. Art. 10 RL 95/46/EG nicht.

Das gilt jedenfalls für diejenigen Besucher von Facebook-Fanpages, die keine Mitglieder des Netzwerkes sind. Beim Aufruf der Seite erhalten sie keine Informationen darüber, dass Cookies gesetzt werden und dass mit deren Hilfe Daten zu Werbezwecken über die Besucher erhoben werden.

Anders als Facebook meint (Schriftsatz vom 31.05.2013, S. 9 -13) willigen aber auch die Besucher von Fanpages, die zugleich Facebook-Mitglieder sind, nicht wirksam mit der Registrierung in die Datenverwendung für „Facebook-Insights" ein. Facebook trägt hierzu vor, dass Nutzer über die Datenverwendungsrichtlinien umfassend darüber informiert würden, welche Daten im Rahmen der Nutzung des Facebook-Netzwerks erhoben und wie und wozu diese Daten verwendet werden. Dieser Darstellung kann nicht gefolgt werden (Welche hohen Anforderungen die Richtlinie an die Einwilligung zum Behavioral Advertising bei Sozialen Netzwerken stellt, zeigt die Art. 29 Datenschutzgruppe, WP 187, S. 22). In den „Datenverwendungsrichtlinien" und den „Nutzungsbedingungen" von Facebook (Anlagen Bg 5, 6 und 7 im Schriftsatz von Facebook vom 31.05.2013) wird der Dienst „Facebook Insights" weder erwähnt, noch beschrieben. Die Ausführungen in den Datenverwendungsrichtlinien sind allgemein und unbestimmt gehalten. Der Nutzer erhält im Rahmen des Registrierungsprozesses keine deutlichen Informationen dazu, ob, wie und auf welche Weise seine Registrierungsdaten (Familienname, Vorname, Geburtsdatum, Geschlecht, E-Mail-Adresse/Mobiltelefonnum-mer) mit den Nutzungsdaten (z.B. IP- und Cookie-Informationen) verknüpft und weiterverarbeitet werden. Dies ist gerade vor dem Hintergrund zu sehen, dass viele Minderjährige das Facebook-Portal nutzen und zu deren Schutz eine transparente Aufklärung stattfinden müsste. Die Datenverwendungsrichtlinien sind zudem nicht verständlich formuliert und räumen Facebook scheinbar umfassende „Verarbeitungsrechte" ein, ohne dass der Nutzer den Umfang der Verarbeitung erfassen kann. Solche pauschalen Einwilligungen widersprechen aber der von Art. 6 Abs. 1 a) RL 95/46/EG geforderten Datenverarbeitung nach „Treu und Glauben" (siehe auch Art. 8 Abs. 2 Satz 1 EU-GrCh), wonach der Betroffene in der Lage sein muss, das Vorhandensein einer Verarbeitung zu erfahren und ordnungsge-

mäß und umfassend über die Bedingungen der Erhebung informiert zu werden (Erwägungsgrund 38 RL 95/46/EG). Vor diesem Hintergrund betrachtet, ist eine solche pauschale Einwilligung unwirksam, da sie nicht für den konkreten Fall im Sinne von Art. 2 h) RL 95/46/EG erfolgt (Art. 29 Datenschutzgruppe, WP 187, S. 20).

Der Dienst „Facebook-Insights" verstößt zudem gegen Art. 5 Abs. 3 Satz 1 RL 2002/58/EG in der durch Art. 2 Ziffer 5 RL 2009/135/EG geänderten Fassung (umgesetzt in Irland durch Sec. 5. (3) der European Communities Regulations 2011). Demnach darf die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet werden, wenn der betreffende Teilnehmer oder Nutzer „auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie 95/46/EG u.a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat." Wie ausgeführt, erhält der Nutzer keine klaren und umfassenden Informationen über den Einsatz des „datr-Cookie", des „fr-Cookie" und sämtlicher anderer Cookies, insbesondere nicht zum Zweck der Verarbeitung (zu den Anforderungen: Art. 29 Datenschutzgruppe, WP 208, S. 3 ff.). Bereits hieran scheitert eine Einwilligung in das Setzen der Cookies, die die Voraussetzungen aus Art. 2 h) RL 95/46/EG erfüllt.

(2) Für die Datenverarbeitung im Rahmen von „Insights" kann sich Facebook auch auf keine der gesetzlichen Erlaubnisgründe des irischen Datenschutzrechts berufen.

Auch die Voraussetzungen von Sec. 2A (1) (b) (i) Data Protection (Amendment) Act 2003 liegen nicht vor. Dieser bestimmt, dass die Datenverarbeitung zulässig ist, wenn dies für die Erfüllung eines Vertrags erforderlich ist:

> *"Processing of personal data.*
>
> *2A. (1) Personal data shall not be processed by a data controller unless section 2 of this Act (as amended by the Act of 2003) is complied with by the data controller and at least one of the following conditions is met:*
>
> *(b) the processing is necessary*
>
> *(i) for the performance of a contract to which the data subject is a party,"*

Mit dieser Norm setzt das irische Recht Art. 7 b) 1. Fall RL 95/46/EG um. Auch nach dieser Vorschrift ist zentrale Voraussetzung, dass die Verarbeitung personenbezogener Daten für den Verantwortlichen „erforderlich" ist, um einen Vertrag mit dem Betroffenen zu erfüllen.

Sec. 2A (1) (b) (i) Data Protection (Amendment) Act 2003 i.V.m. Art. 7 b) 1. Fall RL 95/46/EG scheidet als Erlaubnisgrund aus, da die Datenverarbeitungsprozesse im Rahmen von Facebook-Insights nicht für Facebook erforderlich sind, um eine vertraglich geschuldete Leistung gegenüber den Betroffenen zu erbringen.

Für diejenigen Besucher der Fanpages, die keine Facebook-Mitglieder sind, scheidet dieser Erlaubnisgrund aus, weil Facebook mit ihnen keine vertragliche Beziehung unterhält.

Zwischen Facebook-Mitgliedern und Facebook dagegen mag zwar ein vertragsähnliches Nutzungsverhältnis bestehen. Die Mitglieder verwenden das Portal aber primär, um sich mit anderen Nutzern auszutauschen. Um die dazu nötigen Funktionen bereit zu stellen, ist es aber nicht erforderlich, Registrierungs- (Familienname, Vorname, Geburtsdatum, Geschlecht, E-Mail-Adresse/Mobiltelefonnummer) und Nutzungsdaten der Fanpage (z. B. IP- und Cookieinformationen) im Rahmen von Facebook „Insights" auszuwerten und damit zu verarbeiten. Diese Daten nutzt Facebook vielmehr außerhalb der Nutzungsverhältnisse und gibt sie unter anderem als Statistiken per „Insights" an die Fanpagebetreiber weiter. Um die Kommunikationsfunktionen den Mitgliedern bereit zu stellen, ist es auch nicht erforderlich, dass Facebook zahlreiche Cookies auf den informationstechnischen Systemen der Nutzer setzt, die mehrere Jahre aktiv sind. Der datr-Cookie etwa bleibt zwei Jahre auf den Geräten gespeichert und liefert solange Facebook Informationen. Mit Sicherheitsbedürfnissen kann diese lange Speicherdauer jedenfalls nicht gerechtfertigt werden, da Authentifizierungstoken auch bei deutlich kürzeren Speicherzeiten gleichermaßen die Bedienbarkeit des Netzwerkes und die Sicherheitsbedürfnisse des Anbieters sichern würden (vgl. dazu Art. 29 Datenschutzgruppe, WP 194, S. 7).

(3) Auch auf Sec. 2A (1) (d) kann Facebook die Datenverarbeitung für „Insights" nicht stützen. Nach dieser Vorschrift darf der Verantwortliche Daten verarbeiten, soweit dies zur Wahrnehmung berechtigten Interessen des Verantwortlichen oder eines Datenempfänger erforderlich ist und die Rechte Dritter dem nicht entgegenstehen:

> "Processing of personal data.
>
> 2A. (1) Personal data shall not be processed by a data controller unless section 2 of this Act (as amended by the *Act of 2003*) is complied with by the data controller and at least one of the following conditions is met:
>
> (*d*) the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject."

Dem entspricht Art. 7 f) RL 95/46/EG. Als Erlaubnisgrund scheidet Sec. 2A (1) (d) Data Protection (Amendment) Act 2003 in Verbindung mit Art. 7 f) RL 95/46/EG aus, da kein berechtigtes Interesse auf Seiten von Facebook erkennbar ist, dass gegenüber den Grundrechten der Betroffenen überwiegt. Dem wirtschaftlichen Interesse Facebooks stehen schwere Eingriffe in das Recht Schutz der personenbezogenen Daten gegenüber (Art. 8 EU-GrCh). Der von Facebook vorgenommene Eingriff erfolgt auch nicht im Rahmen der von Art. 8 Abs. 2 Satz 1 EU-GrCh vorgesehenen Grenzen, da die Verarbeitung jedenfalls nicht nach „Treu und Glauben" erfolgt (vgl. Erwägungsgrund 38 RL 95/46/EG). Die Betroffenen erhalten nämlich keine Informationen darüber, dass sowohl ihre Registrierungsdaten (soweit bei Facebook-Mitgliedern vorhanden), als auch die mit den Cookies gewonnenen Nutzungsdaten für Werbezwecke im Rahmen von Facebook „Insights" verarbeitet werden. In diesem intransparenten Umfeld sind die Betroffenen vielmehr nicht in der Lage zu erfahren, welche Daten über sie erhoben und zu welchen Zwecken diese verarbeitet werden.

bb) Objektive Vorhersehbarkeit der Datenschutzverstöße

Dass der Betrieb der Fanpage durch die Berufungsbeklagte zu den aufgezeigten Datenschutzverstößen führt, ist auch objektiv vorhersehbar. Das Verhalten der Berufungsbeklagten und die von Facebook vorgenommene datenschutzrechtswidrige Verarbeitung der Nutzungsdaten bilden eine natürliche Handlungseinheit, weil diese Störung typische Folge der Handlungen der Berufungsbeklagten ist.

Indem die Berufungsbeklagte durch die von ihr eingestellten Inhalte Nutzer auf ihre Fanpage zieht, werden deren Verhalten im Rahmen von Facebook datenschutzrechtswidrig erfasst. Zudem werden in aller Regel auf den Systemen der Nutzer Cookies gesetzt, sodass typischerweise deren Surfverhalten im Internet auch über die Plattform hinaus getrackt wird. Wer den Ausführungen zur Verantwortlichkeit (unter B.) nicht folgt, mag den Betrieb der Fanpage zwar als neutrale Handlung ansehen. Für jeden unbeteiligten Dritten ist aber augenscheinlich, dass dieser Beitrag letztlich dazu führt, dass das Verhalten der Nutzer der Fanpage durch Facebook erfasst und diese Daten zur Profilbildung in datenschutzrechtswidriger Weise verwendet werden. Facebook betreibt diese Infrastruktur bekanntlich, um zielgruppenorientierte Werbung zu vermarkten. Das ist der Kern des von Facebook sehr erfolgreich betriebenen Geschäftskonzepts. In diesem Geschäftskonzept nehmen die Fanpagebetreiber eine zentrale Rolle ein, da sie das Netzwerk mit Inhalten füllen. Deshalb besteht zwischen Facebook und den Fanpagebetreibern ein enges Kooperationsverhältnis. Dieses Kooperationsverhältnis bildet eine natürliche Einheit, die es rechtfertigt, die Nutzungsdatenverarbeitung auch der Berufungsbeklagten zuzurechnen.

Darüberhinaus hat die Berufungsbeklagte den aufgezeigten Störungszustand auch subjektiv bezweckt. Sie hat als Kooperationspartnerin von Facebook das Errichten der Fanpage mit dem Ziel verbunden, aus den rechtswidrig erhobenen Nutzerdaten eine für eigene Werbezwecke wertvolle anonymisierte Nutzerstatistik zu erhalten. Ein Verschulden ist hierfür nicht erforderlich (Volkmann, Der Störer im Internet, Schriftenreihe Information und Recht, Band 54, 2005, S. 206). In diesem Zusammenhang hat sie auch ihre Prüfpflichten verletzt, zumal bereits vor der streitgegenständlichen Anordnung des ULD vom 03.11.2011 mit Pressemitteilung des ULD vom 19.08.2011 und mit Schreiben des ULD vom 05.10.2011 die Berufungsbeklagte über die datenschutzrechtliche Beurteilung des Betriebs einer Facebook-Fanpage informiert wurde und diese einen Weiterbetrieb der Fanpage gleichwohl vornahm.

Die Berufungsbeklagte hat zudem die Möglichkeit, die rechtswidrige Verarbeitung personenbezogener Nutzerdaten durch Facebook zu verhindern, indem sie die Fanpage nicht betreibt. Sie hat lediglich vorgetragen, dass ihr der Betrieb der Fanpage wichtig sei, da sie andernfalls im Vergleich zu konkurrierenden Bildungsträgern Wettbewerbsnachteile zu befürchten habe (Schriftsatz der Klägerin und Berufungsbeklagten vom 19.01.2012, S. 2 f.). Die Berufungsbeklagte trägt aber nicht konkret vor, welche messbaren wirtschaftlichen Vorteile ihr der Betrieb der Fanpage bringt. Schwerwiegende Beeinträchtigungen der aus den Art. 16 und 17 EU-GrCh folgenden Rechte hat sie nicht dargelegt. Hingegen werden die Rechte der Nutzer aus Art. 8 Abs. 1 EU-GrCh eklatant verletzt, da sie sich gegen eine Verarbeitung ihrer personenbezogenen Daten für Werbezwecke nicht zur Wehr setzen können. Von den Nutzern werden bezüglich der Datenverarbeitung keine rechtswirksamen Einwilligungen eingeholt und es bestehen keine Möglichkeiten einer entsprechenden Datenverarbeitung zu widersprechen.

D. Haftung der Wirtschaftsakademie Schleswig-Holstein GmbH als Diensteanbieter

Von mehreren Gerichten wurde anerkannt, dass Facebook-Fanpagebetreiber Diensteanbieter im Sinne des TMG sind und das TMG auf diese anwendbar ist (LG Aschaffenburg Urteil vom 19.08.2011 – 2 HK O 54/11; OLG Düsseldorf I, Urteil vom 13.08.2013 – 20 U 75/13). Nach § 2 S. 1 Nr. 1 TMG sind Diensteanbieter natürliche und juristische Personen, die eigene oder fremde Telemedien zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln. Bei Fanpagebetreibern kommt es nicht darauf an, ob sie Telemedien ausschließlich selbst anbieten oder dies vermittelt über einen Zugang zu Facebook tun. Auf jeden Fall gelten für sie auch die Regelungen des TMG für Diensteanbieter.

Entgegen der Ansicht des VG Schleswig ist damit für Fanpagebetreiber als Diensteanbieter § 15 Abs. 3 TMG relevant. Dieser erlaubt Diensteanbietern bzw. den durch sie vermittelten Diensten zwar grundsätzlich Nutzungsdaten der Besucher zur Profilbildung zu verwenden. Jedoch muss dies unter Pseudonym erfolgen und die Besucher der Fanpage müssen eine Widerspruchsmöglichkeit haben. Bei Facebook-Fanpages erfolgt die Profilerstellung in Verbindung mit dem Facebookprofil des Nutzers. Dieses wiederum muss nach den Facebook-Richtlinien den Klarnamen des Nutzers zwingend enthalten und darf kein Pseudonym sein. Auch hat der Nutzer keine Möglichkeit der Profilerstellung zu widersprechen.

Die Nutzer besuchen hierbei ausdrücklich nicht nur die Telemedien von Facebook, sondern bewusst und gezielt die Fanpage, die die Berufungsbeklagte als Diensteanbieter betreibt. Sie ist verpflichtet die Vorgaben des § 15 Abs. 3 TMG einzuhalten, auch wenn sie sich Facebook als weiteren Dienstleister für die Bereitstellung der Inhalte bedient. Diese Vorgaben werden hier jedoch erkennbar nicht beachtet, weshalb der Betrieb der Fanpage rechtswidrig ist.

Der Berufung ist daher in vollem Umfang stattzugeben.

E. Vorabentscheidungsverfahren nach Art. 267 AEUV

Abschließend bleibt festzuhalten, dass nach unserer Auffassung zwei Fragen über den Ausgang dieses Verfahrens entscheiden. Zum einen hängt der Ausgang des Rechtsstreits von den Voraussetzungen der Verantwortlichkeit nach § 3 Abs. 7 BDSG und zum anderen von dem vermeintlich abschließenden Charakter des Datenschutzrechts gegenüber den allgemeinen Haftungsregeln ab.

Beide Fragen werden durch die weitgehend zwingenden Vorgaben aus der Richtlinie 95/46/EG determiniert. Sollte das erkennende Gericht nicht der von uns vertretenen Auslegung des europäischen Rechts folgen, regen wir angesichts der Bedeutung der Rechtsfragen und dem Charakter dieses Verfahrens als Musterprozess an, das Verfahren auszusetzen und diese Fragen zur Vorabentscheidung gemäß Art. 267 AEUV dem Europäischen Gerichtshof wie folgt vorzulegen:

> 1. Ist Art. 2 lit. d) der Richtlinie 95/46/EG dahingehend auszulegen, dass im Falle eines Netzwerks, das Dritten die Möglichkeit bietet, innerhalb des Netzwerks eine Internetseite anzulegen und zu betreiben, und die Aktivitäten von Nutzern der Internetseite durch Verarbeitung deren personenbezogener Daten nachverfolgt, auswertet und die Ergebnisse dieser Auswertung den Betreibern der Internetseite in aggregierter und anonymisierter Form zur Verfügung stellt, allein die Entscheidung eines Dritten zur Anlage einer Internetseite in diesem Netzwerk genügt, um diesen zum datenschutzrechtlich für die Verarbeitung Verantwortlichen zu qualifizieren?

2. Falls die erste Frage verneint werden sollte: Steht die Richtlinie 95/46/EG einer Regelung im nationalen Recht entgegen, durch die nicht nur der für die Verarbeitung Verantwortliche auf Unterlassung seiner Handlungen in Anspruch genommen werden kann, sondern auch weitere Personen, die einen kausalen Beitrag zu dem Datenschutzverstoß leisten, die eine andere Person begeht?

Mit freundlichem Gruß

Dr. Thilo Weichert