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, 21. Juli 2014

Verwaltungsrechtssache Unabhängiges Landeszentrum für Datenschutz ./. Wirtschaftsakademie Schleswig-Holstein GmbH
4 LB 20/13, Ihr Schreiben vom 16. Juni 2014

Sehr geehrte Damen und Herren,

in vorbezeichneter Angelegenheit erwidern wir auf das Schreiben der Berufungsbeklagten und erlauben uns, aufgrund der zwischenzeitlich auf Bundes- sowie Unionsebene ergangenen Rechtsprechung noch einmal geordnet zur Rechtmäßigkeit der Anordnung und damit zur Fehlerhaftigkeit der Entscheidung des Verwaltungsgerichts Stellung zu nehmen. Entscheidend für die tatsächliche und rechtliche Beurteilung ist, dass Facebook gegen geltendes Datenschutzrecht verstößt (dazu unter 1.) und die Berufungsbeklagte für die Verstöße verantwortlich ist (dazu unter 2.).

1. Für Facebook gilt deutsches Datenschutzrecht, insbesondere das TMG. Dieser Schluss folgt aus den Wertungen, die der EuGH im Urteil vom 13. Mai 2014, Az.: C-131/12, aufgestellt hat. Die Facebook Inc. muss deutsches Datenschutzrecht, insbesondere die Regelungen des TMG, beachten, denn Facebook Inc. betreibt in Deutschland mit der Facebook Germany GmbH, Großer Burstah 50-52, 20457 Hamburg, eine Niederlassung im Sinne von Art. 4 Abs. 1 a) der Richtlinie 95/46/EG. Die Facebook Germany GmbH wurde 2009 in Hamburg eröffnet, „um die Zusammenarbeit von Marken und Unternehmen mit Kunden oder Fans auf Facebook zu verbessern“ (Quelle: www.firmendb.de/firmen/6781166.php). Ähnliche Feststellungen hat die irische Datenschutzaufsichtsbehörde getroffen (Facebook Ireland Ltd., Report of Audit vom 21. Dezember 2011, S. 28):

„Inside Sales Operations also handle the management of advertising accounts with associated interaction with local offices (Facebook France, Facebook Germany, etc.) and is responsible for bringing new business to Facebook through generating new sales leads."

Die Facebook Germany GmbH unterstützt durch Werbe- und Marketingmaßnahmen die Nutzung der Facebook-Dienste. Diese Tätigkeit ist ausreichend, um die Facebook Germany GmbH als Niederlassung nach Art. 4 Abs. 1 a) der Richtlinie 95/46/EG zu qualifizieren. Es ist hierfür nicht notwendig, dass die Facebook Germany GmbH selbst personenbezogene Daten verarbeitet. Art. 4 Abs. 1 a) der Richtlinie 95/46/EG verlangt nicht, dass die Verarbeitung personenbezogener Daten „von" der betreffenden Niederlassung selbst ausgeführt wird, sondern lediglich, dass sie „im Rahmen der Tätigkeiten" der Niederlassung ausgeführt wird (EuGH, Urteil vom 13. Mai 2014, Az.: C-131/12, BeckRS 2014, 80862, Rz. 34). Zur Tätigkeit einer spanischen Niederlassung der Google Inc. hat der EuGH ausgeführt (BeckRS 2014, 80862, Rz. 55):

„Im Hinblick auf dieses Ziel der Richtlinie 95/46 und den Wortlaut ihres Art. 4 Abs. 1 Buchst. a ist davon auszugehen, dass die Verarbeitung personenbezogener Daten, die für den Dienst einer Suchmaschine wie Google Search erfolgt, die von einem Unternehmen betrieben wird, das seinen Sitz in einem Drittstaat hat, jedoch in einem Mitgliedstaat über eine Niederlassung verfügt, „im Rahmen der Tätigkeiten" dieser Niederlassung ausgeführt wird, wenn diese die Aufgabe hat, in dem Mitgliedstaat für die Förderung des Verkaufs der angebotenen Werbeflächen der Suchmaschine, mit denen die Dienstleistung der Suchmaschine rentabel gemacht werden soll, und diesen Verkauf selbst zu sorgen."

Sollte dieser Wertung nicht gefolgt werden, ist deutsches Datenschutzrecht jedenfalls anwendbar, weil die amerikanische Facebook-Konzernmutter in Deutschland personenbezogenen Daten verarbeitet und die Anwendung deutschen Datenschutzrechts nicht gemäß § 1 Abs. 5 Satz 1 Halbsatz 1 BDSG durch irisches Datenschutzrecht ausgeschlossen wird. So entschied das Kammergericht Berlin mit Urteil vom 24.01.2014 (Az. 5 U 42/12):

„Vorliegend ist deutsches Datenschutzrecht anzuwenden […] Die für den hier maßgeblichen Internetauftritt in Deutschland verwendeten Server und Anlagen werden im Ausgangspunkt von der Muttergesellschaft der Beklagten in den USA - also außerhalb des EWR - vorgehalten. Ebenso werden die über den Internetauftritt der Beklagten erhobenen und weitergehend verwendeten Daten in tatsächlicher Hinsicht von dieser Muttergesellschaft verarbeitet. […] Das somit - im Ausgangspunkt - anwendbare deutsche Datenschutzrecht wird nicht gemäß § 1 Abs. 5 Satz 1 Halbsatz 1 BDSG durch irisches Datenschutzrecht ausgeschlossen. […]Dass die Beklagte eine "feste Einrichtung" ist, steht außer Frage. ~s fehlt aber ein hinreichender Vortrag dazu, dass sie die hier maßgebliche Erhebung und weitere Verarbeitung der Daten vornimmt. Insoweit ist § 1 Abs. 5 BDSG richtlinienkonform dahin auszulegen, dass diese Datenverarbeitungsvorgänge von der Beklagten auch "effektiv und tatsächlich" ausgeübt wird. […]Unabhängig davon ist deutsches Datenschutzrecht vorliegend auch vertragsrechtlich aufgrund einer Rechtswahl der Vertragsparteien (Beklagte und Nutzer) maßgeblich."

Zusätzlich zu den Verstößen gegen das deutsche TMG verstößt Facebook auch durch die unkontrollierte und intransparente Weitergabe von personenbezogenen Daten an nationale Geheimdienste in den USA und Großbritannien gegen geltendes Datenschutzrecht. In diesem Zusammenhang hat

der irische High Court in seiner Entscheidung vom 18. Juni 2014 im Verfahren Maximilian Schrems gegen den Irischen Datenschutzbeauftragten (abrufbar unter http://www.europe-v-facebook.org/hcj.pdf) ausgeführt, dass die dank Edward Snowden bekannt gewordenen massenhaften Datenabfragen bei Facebook die Datenschutzrechte der Nutzer verletzten. Diese Verstöße sind dabei derart eklatant, dass der irische High Court dem EuGH die Frage zur Entscheidung vorgelegt hat, ob vor dem Hintergrund dieser Erkenntnisse die Safe Harbor Entscheidung der Europäischen Kommission (Amtsblatt der EG vom 28. Mai 2000, 2000/520/EG) Bestand haben kann:

76. Third, the evidence suggests that personal data of data subjects is routinely accessed on a mass and undifferentiated basis by the US security authorities … (ebenso Rn. 13.).

In Rn. 45 stellt das Gericht klar, dass für einen Betroffenen die Datenweitergabe an die USA grundrechtsrelevant ist: … *he is nonetheless certainly entitled to object to a state of affairs where his data are transferred to a jurisdiction which, to all intents and purposes, appears to provide only a limited protection against any inference with that private data by US security authorities.*

Das irische Gericht weist darauf hin, dass die erfolgende Massenüberwachung angesichts der Rechtsprechung des EuGH zur Vorratsdatenspeicherung (U. v. 8. April 2014, C-293/12 und C-594/12, abgedruckt z. B. in DVBl 2014, 708 = DuD 2014, 488) sowohl gegen europäische Grundrechte (Art. 7, 8 Europäische Grundrechte-Charta, (Rn. 58 ff.) wie auch gegen die irische Verfassung verstößt.

78. Fifth, the chief constitutional protections are those relating to personal privacy and the inviolability of the dwelling. The general protection for privacy, person and security which is embraced by the „inviolability" of the dwelling in Art40.5 of the Constitution would be entirely compromised by the mass and undifferentiated surveillance by State authorities of conversation and communications which take place within the home.

Damit ist in jeder Hinsicht eindeutig, dass die derzeitigen Datenverarbeitungen bei Facebook gegen geltendes Datenschutzrecht in Deutschland und Europa verstoßen. Die derzeitige Praxis der Profilbildung sowie die Cookie-Nutzung sind wegen Verstoßes gegen das TMG rechtswidrig. Die tiefgreifende Ausforschung durch die US-amerikanischen Geheimdienste ist daneben ein evidenter Verstoß gegen Grundprinzipien der informationellen Selbstbestimmung.

Für die Frage der durch Facebook herbeigeführten Datenschutzverstöße ist in tatsächlicher Hinsicht relevant, welche Daten Facebook über Mitglieder (eingeloggt und nicht eingeloggt) sowie Nicht-Mitglieder erhebt und wie diese genutzt werden. Dazu wurde bereits im erstinstanzlichen Verfahren ausgeführt und in der Berufungsbegründung ergänzt. Zusammenfassend lässt sich hierzu Folgendes feststellen:

Eingeloggte Mitglieder

Facebook erhebt Nutzungsdaten und verbindet diese mit nicht pseudonymisierten Profildaten. Technisch erfolgt dies über Cookies, die beim Besuch auf den Fanpages gesetzt werden. Dieses Zusammenführen ist ein Verstoß gegen § 15 Abs. 3 Satz 3 TMG. Daneben fehlt es an einer Möglichkeit zum Widerspruch nach § 15 Abs. 3 Satz 2 TMG i. V. m. § 13 Abs. 1 TMG. Die im Rahmen der Nut-

zungsvereinbarung abgegebene Einwilligung ist nicht wirksam, weil der Nutzer nicht ausreichend informiert wird und kein Widerspruch möglich ist.

Nicht eingeloggte Mitglieder

Bereits ausführlich begründet wurde, dass Facebook seine Nutzer auch ohne Anmeldung über den datr-Cookie erkennt und hierzu Daten sammelt.

Nicht-Mitglieder

Auf den Rechnern von Nicht-Mitgliedern werden Cookies durch Facebook gesetzt, ohne dass irgendwelche Sicherheitsvorkehrungen getroffen würden. Cookies sind den Nutzungsdaten zuzurechnen (Voigt, MMR 2009, 377ff. (381)) und unterfallen daher dem Vorbehalt des § 15 Abs. 1 TMG. Da die Cookies in der eingesetzten Form nicht für die Nutzung erforderlich sind (vgl. datr-Cookie mit einer Lebenszeit von zwei Jahren), sind sie unzulässig; ihre Verwendung stellt einen Verstoß gegen deutsches Datenschutzrecht dar.

2. Für diese Rechtsverletzungen ist die Berufungsbeklagte auch verantwortlich. Dies folgt aus der Anwendung der Richtlinie 95/46/EG durch Wahl von Facebook als Anbieter für die Fanpages (Mittel) und der Entscheidung, die Facebook-Infrastruktur zur Kommunikation mit Kunden und Interessierten zu nutzen und gleichzeitig Erkenntnisse über das Zielpublikum zu erhalten (Zweck). Diese bereits im erstinstanzlichen Verfahren ausführlich dargelegte Rechtsposition wird durch die oben erwähnte jüngste Rechtsprechung des EuGH bestätigt:

a) Für die Beurteilung von Bedeutung ist die Entscheidung des EuGH vom 13. Mai 2014, Az.: C-131/12, in welcher zur datenschutzrechtlichen Verantwortlichkeit von Suchmaschinenbetreibern Stellung bezogen wird. Demnach ist Art. 2 b) und d) der Richtlinie 95/46/EG dahin auszulegen, dass die Tätigkeit einer Suchmaschine, die darin besteht, von Dritten ins Internet gestellte oder dort veröffentlichte Informationen zu finden, automatisch zu indexieren, vorübergehend zu speichern und schließlich den Internetnutzern in einer bestimmten Rangfolge zur Verfügung zu stellen, sofern die Informationen personenbezogene Daten enthalten, als „Verarbeitung personenbezogener Daten" im Sinne von Art. 2 b) der Richtlinie 95/46/EG einzustufen und dass der Betreiber dieser Suchmaschinen als für diese Verarbeitung „Verantwortlicher" im Sinne von Art. 2 d) der Richtlinie 95/46/EG anzusehen ist. Der EuGH führt in diesem Zusammenhang aus (BeckRS 2014, 80862, Rz. 38-40):

„Durch die Tätigkeit einer Suchmaschine können die Grundrechte auf Achtung des Privatlebens und Schutz personenbezogener Daten somit erheblich beeinträchtigt werden, und zwar zusätzlich zur Tätigkeit der Herausgeber von Websites; als derjenige, der über die Zwecke und Mittel dieser Tätigkeit entscheidet, hat der Suchmaschinenbetreiber daher in seinem Verantwortungsbereich im Rahmen seiner Befugnisse und Möglichkeiten dafür zu sorgen, dass die Tätigkeit den Anforderungen der Richtlinie 95/46 entspricht, damit die darin vorgesehenen Garantien ihre volle Wirksamkeit entfalten können und ein wirksamer und umfassender Schutz der betroffenen Personen, insbesondere ihres Rechts auf Achtung ihres Privatlebens, tatsächlich verwirklicht werden kann.

Schließlich ist festzustellen, dass der Umstand, dass die Herausgeber von Websites die Möglichkeit haben, den Suchmaschinenbetreibern u. a. mit Hilfe von Ausschlussprotokollen wie „robot.txt" oder Codes wie „noindex" oder „noarchive" zu signalisieren, dass eine bestimmte auf ihrer Website veröffentlichte Information ganz oder teilweise von den automatischen Indexen der Suchmaschinen ausgeschlossen werden soll, nicht bedeutet, dass das Fehlen eines solchen Hinweises seitens der Herausgeber von Websites den Suchmaschinenbetreiber von seiner Verantwortung für die von ihm im Rahmen der Tätigkeit der Suchmaschinen vorgenommene Verarbeitung personenbezogener Daten befreite.

Dies ändert nämlich nichts daran, dass der Suchmaschinenbetreiber über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Selbst wenn die genannte Möglichkeit der Herausgeber von Websites bedeuten sollte, dass sie gemeinsam mit dem Suchmaschinenbetreiber über die Mittel der Verarbeitung personenbezogener Daten entscheiden, nimmt dies dem Suchmaschinenbetreiber nichts von seiner Verantwortung, da Art. 2 Buchst. d der Richtlinie 95/46 ausdrücklich vorsieht, dass die Entscheidung über die Mittel „allein oder gemeinsam mit anderen" erfolgen kann."

Der EuGH zieht in der erwähnten Entscheidung deutlich in Erwägung, dass der Suchmaschinenbetreiber und der jeweilige Webseitenbetreiber gemeinsam über die Mittel der Datenverarbeitung entscheiden. Dabei ist zu berücksichtigen, dass zwischen dem Suchmaschinenbetreiber und dem Webseitenbetreiber nicht einmal eine Nutzungsvereinbarung oder eine andere vertragliche Abrede besteht. Regelmäßig signalisieren die Webseitenbetreiber (z. B. mittels Ausschlussprotokollen wie „robot.txt" oder Codes wie „noindex" oder „noarchive") dem Suchmaschinenbetreiber kaum, welche veröffentlichten Inhalte von den automatischen Indexen der Suchmaschinen ausgeschlossen sein sollen. Gleichwohl hält der EuGH eine gemeinsame datenschutzrechtliche Verantwortlichkeit von Suchmaschinenbetreiber und Webseitenbetreiber möglich, was wiederum zeigt, dass an die Annahme einer gemeinsamen Verantwortlichkeit keine hohen Anforderungen gestellt werden dürfen. Allein die technische Option, durch Ausschlussprotokolle oder Codes eine Indexierung durch den Suchmaschinenbetreiber zu verhindern, kann daher zur Annahme einer datenschutzrechtlichen Verantwortlichkeit von Suchmaschinenbetreiber und Webseitenbetreiber führen, da diese gemeinsam über die verwendeten Mittel entscheiden.

Führt bereits dieses Zusammenwirken zwischen Suchmaschinenbetreiber und Webseitenbetreiber zur Annahme einer gemeinsamen datenschutzrechtlichen Verantwortlichkeit, so trifft dies für die dargelegte Kooperation zwischen Facebook und der Berufungsbeklagten erst recht zu. Zwischen Facebook und der Berufungsbeklagten besteht eine vertragliche Vereinbarung zum Betrieb einer Fanpage. Mittels der Fanpage wird es Facebook gezielt ermöglicht, die mehrfach erwähnten Nutzungsinformationen von den Nutzern bzw. Besuchern der Fanpage zu erheben, für Werbezwecke zu verarbeiten und zu nutzen. Die Berufungsbeklagte erhält auf Basis der Vereinbarung mit Facebook eine anonymisierte Nutzungsstatistik, deren Erstellung erst durch die Erhebung der personenbezogenen Nutzungsinformationen über die Fanpage möglich wurde. Mit dem Anlegen oder Außer-Betrieb setzen/Löschen der Fanpage steuert die Berufungsbeklagte die Erhebung der personenbezogenen Daten der Nutzer durch Facebook. Die Verzahnung der Tätigkeiten zwischen der Berufungsbeklagten und Facebook ist deutlich stärker ausgeprägt als im Verhältnis zwischen Suchmaschinenbetreiber und Webseitenbetreiber. Facebook stellt potentiellen Fanpagebetreibern eine technische Infrastruktur zum Betrieb von Fanpages bereit und möchte die Fanpagebetreiber vertraglich an sich binden. Die Berufungsbeklagte ermöglicht mit dem Anlegen der Fanpage die

Realisierung des Geschäftskonzepts und profitiert von den Analyseergebnissen aus dem Dienst Facebook Insights. Eine derart enge Bindung zwischen Suchmaschinenbetreiber und Webseitenbetreiber ist nicht erkennbar. Vor allem bietet der Suchmaschinenbetreiber dem Webseitenbetreiber keine Infrastruktur zum Anlegen eigener Webseiten, gekoppelt mit der Abrede, dass eine Indexierung vorgenommen wird. Der Webseitenbetreiber erlangt auch keine vertraglich vereinbarten Vorteile aus einem Dienst, der mit Facebook Insights vergleichbar ist. Gleichwohl sieht der EuGH eine gemeinsame Verantwortlichkeit des Suchmaschinenbetreibers und des Webseitenbetreibers als gegeben an.

b) Weiterhin stellt der EuGH in seiner Entscheidung klar, dass die datenschutzrechtliche Verantwortlichkeit keine Kontrolle über die personenbezogenen Daten voraussetzt (BeckRS 2014, 80862, Rz. 34):

„Im Übrigen ließe es sich nicht nur nicht mit dem klaren Wortlaut, sondern auch nicht mit dem Ziel der genannten Bestimmung, durch eine weite Bestimmung des Begriffs des „Verantwortlichen" einen wirksamen und umfassenden Schutz der betroffenen Personen zu gewährleisten, vereinbaren, den Suchmaschinenbetreiber deshalb von diesem Begriff auszunehmen, weil die auf den Internetseiten Dritter veröffentlichten personenbezogenen Daten nicht seiner Kontrolle unterliegen."

Der Suchmaschinenbetreiber erhebt in diesem Zusammenhang personenbezogene Daten unabhängig davon, ob eine besondere Verfügungsmacht hierzu besteht (anders noch OLG Hamburg, Beschluss vom 13.11.2009, 7 W 125/09). Unrichtig wäre es auch, für die datenschutzrechtliche Verantwortlichkeit der Berufungsbeklagten eine besondere Verfügungsbefugnis zu verlangen.

Ein Erheben ist erfolgt, sobald die Stelle eine eigene Verfügung über die Daten begründet hat. Dazu genügt es, wenn eine für die erhebende Stelle handelnde Person Datenträger in Besitz oder Daten zur Kenntnis genommen hat. Eine Vollmacht ist dafür nicht erforderlich (Dammann, in: Simitis, BDSG, 7. Auflage 2011, § 3 Rn. 107). Es reicht aus, wenn Facebook zur Erfüllung der Kooperation mit der Wirtschaftsakademie bzw. zur Bereitstellung der aus personenbezogenen Daten generierten Nutzungsstatistik personenbezogene Daten erhebt. Dieses Handeln einer anderen Stelle kann im Wege der Auftragsdatenverarbeitung oder durch eine andere verantwortliche Stelle im Rahmen einer Vereinbarung erfolgen. Es liegt zugleich eine Eigenerhebung der verantwortlichen Stelle vor, wenn die Erhebung durch eine andere verantwortliche Stelle im Rahmen einer Vereinbarung erfolgt. Dies liegt hier vor, da die Berufungsbeklagte mit Facebook eine Vereinbarung über den Betrieb einer Fanpage nebst Erhebung von Nutzungsdaten getroffen hat. Auch die Bereitstellung von anonymisierten Nutzungsdaten durch Facebook war klarer Vertragsbestandteil.

Weiterhin sind für den Begriff des Erhebens der Anlass der Datenbeschaffung, ihr Zweck und die beabsichtigte oder tatsächliche Verwendung der erhaltenen Informationen irrelevant. Insbesondere braucht nicht die Absicht zu bestehen, die Informationen personenbezogen zu verwenden (so ausdrücklich Dammann, in: Simitis, BDSG, 7. Auflage 2011, § 3 Rn. 105 mit Verweis auf Bergmann/Möhrle/Herb, BDSG, § 3 Rn. 64). Die Berufungsbeklagte hat sich in diesem Zusammenhang deutlich dafür entschieden, die personenbezogenen Daten nur in Form einer anonymisierten Nutzungsstatistik zu verwenden.

Im Übrigen verweisen wir auf unser Vorbringen in der Erstinstanz sowie auf die Ausführungen in unserem Schriftsatz vom 18. Dezember 2013.

Sollte das Gericht weitere Erläuterungen für erforderlich halten, so wird höflich um einen Hinweis gebeten.

Mit freundlichem Gruß

Dr. Thilo Weichert