Dr. Udo Kauß
Rechtsanwalt

RA Dr. Udo Kauß, Herrenstraße 62, 79098 Freiburg

vorab per Telefax 0341/2007-1000
Bundesverwaltungsgericht
Simsonplatz 1

04107 Leipzig

Herrenstraße 62
79098 Freiburg i. B.

Telefon: 0761/702093
Telefax: 0761/702059

13/01/16 ka/ka
14/001043
(Bitte stets angeben)

In dem Verwaltungsrechtsstreit

der Wirtschaftsakademie Schleswig-Holstein GmbH

Az. 1 C 28.14

gegen

das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

Beigeladen: Facebook Ireland Limited Dublin, Ireland

wird in Vorbereitung der mündlichen Verhandlung und in Erwiderung auf den Schriftsatz der Klägerin und Revisionsbeklagten vom 06.05.2015 sowie die Schriftsätze der Beigeladenen vom 12.05. und 20.10.2015 und unter Einbeziehung der jüngsten Rechtsprechung des Europäischen Gerichtshofes in Sachen Schrems (Case C-362/14, Maximillian Schrems v Data Protection Commissioner) vom 06.10.2015 sowie des belgischen Dutch-Speaking Court of First Instance Brussels vom 09.11.2105 ausgeführt:

Die Klägerin und die Beigeladene wenden sich umfangreich sowohl gegen die tatbestandlichen als auch die materiell-rechtlichen Rügen der Revisionsbegründung. Diese Ausführungen geben dazu Anlass, die Eckpunkte der Argumentation des Bekl. noch einmal fokussierend und zusammenfassend darzulegen.

1. Zusammenfassende Darstellung der Argumentation des Beklagten

Gegenstand der strittigen Anordnung ist die Facebook-Seite („Fanpage“) der Klägerin, nicht die Geschäftspraxis der Beigeladenen oder der Facebook Inc. in den USA. Dass trotzdem auch das Geschäftsmodell der Beigeladenen und der Facebook Inc. ausführlich diskutiert wird, begründet sich darin, dass die datenschutzrechtlichen Verstöße, die dem Geschäftsmodell der Beigeladenen und der amerikanischen Konzernmutter zugrunde liegen, Anknüpfungspunkt für den eigenen Rechtsverstoß der Klägerin sind. Diese Verknüpfung ändert aber nichts daran, dass Gegenstand der streitgegenständlichen Anordnung ein eigener Verstoß der Klägerin ist.

Dieser Verstoß liegt in der Beauftragung eines ungeeigneten Anbieters mit der Erstellung, Bereithaltung und Wartung eines Internetauftritts. Die Beigeladene bietet eine Infrastruktur an, die es Unternehmen und sonstigen Gruppierungen erlaubt, einen eigenen Internetauftritt zu erstellen und dort Inhalte zu veröffentlichen. Dieser Internetauftritt ist zwar optisch und funktional einem weitgehend vorgegebenen Design unterworfen, inhaltlich und rechtlich aber jeder anderen Webseite gleichzustellen. Soweit die Klägerin dieses kostenlose Angebot annimmt und von der Beigeladenen erfüllen lässt, ist sie für die dabei anfallenden Datenverarbeitungen im gleichen Maße nach § 3 Abs. 7 BDSG verantwortlich wie für jede andere von einem Dienstleister fremd-gewartete Webseite. Erweist sich ein beauftragter Dienstleister als unfähig oder unwillig zur Einhaltung datenschutzrechtlicher Vorgaben, so sind die Zusammenarbeit mit diesem und die Nutzung des Dienstes zu beenden.

Mit seiner Anordnung hat der Beklagte dementsprechend die Deaktivierung eines Webauftritts bezweckt, dessen Wartung und Unterhaltung durch einen Dienstleister erfolgt, der keine ausreichende Gewähr für die Einhaltung der datenschutzrechtlichen Vorgaben bietet. Die Tatsache, dass die Beigeladene jede Mitsprache an der technischen Gestaltung im Hintergrund ablehnt und sich jeder Weisung hinsichtlich datenschutzrechtlicher Anpassungen verwehrt, vermag die Klägerin nicht zu

entlasten. Diese Tatsache stellt als Verstoß gegen die Grundprinzipien der Auftragsdatenverarbeitung vielmehr einen eigenen gewichtigen Verstoß dar.

Die streitgegenständliche Anordnung bezieht sich dementsprechend mit § 38 Abs. 5 S. 1 BDSG in rechtmäßiger Weise auf die Beseitigung eines Verstoßes der Klägerin, nämlich die Nutzung der Facebook-Infrastruktur als technischer Grundlage ihres Webauftritts.

2. Das Urteil des OVG hält einer Revision nicht stand. Im Einzelnen

2.1. Zur Wahl der Ermächtigungsgrundlage

Das BDSG sieht in § 38 Abs. 5 S. 1 und S. 2 BDSG den Erlass von Anordnungen zur Beseitigung von Mängeln in Verarbeitungsverfahren sowie - als Steigerung - die Untersagung einzelner Verfahren vor. Der Beklagte stützte seine Anordnung mit dem Ziel, dass die

> „Internetseite unter https://www.facebook.com/wirtschaftsakademie deaktiviert wird“

von Anfang an und richtigerweise auf § 38 Abs. 5 S. 1 BDSG. Gegenstand der Anordnung ist nicht die Untersagung eines gesamten Verfahrens, sondern die Behebung eines Mangels innerhalb eines spezifischen Datenverarbeitungsvorgangs der Klägerin. Dieser Mangel lag in der Nutzung der Infrastruktur der Beigeladenen für die Präsentation einer Webseite. Nicht der grundsätzliche Betrieb einer Webseite, sondern der Rückgriff auf die Dienste der Beigeladenen ist Grund für die Anordnung. Dies zeigt sich bereits daran, dass der Betrieb der unter http://www.wak-sh.de/ bereitgehaltenen Webseite von der Anordnung völlig unberührt blieb.

Soweit das Oberverwaltungsgericht im angegriffenen Urteil (US 19) ausführt, dass die Anordnung des Beklagten als Maßnahme nach § 38 Abs. 5 S. 2 BDSG zu bewerten ist und sich der Beklagte zunächst auf § 38 Abs. 5 S. 1 hätte stützen müssen, verkennt es, dass auch jeder Anordnung nach § 38 Abs. 5 S. 1 BDSG notwendigerweise immer eine untersagende Komponente innewohnt.

Die aus § 38 Abs. 5 S. 1 BDSG folgende Befugnis,

> „Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel“

anzuordnen, muss denklogisch auch immer die Untersagung der Fortdauer des festgestellten Verstoßes beinhalten. So war beispielsweise im Urteil des VG Berlin vom 24.05.2011 (1 K 133/10) die Anordnung des Berliner Landesbeauftragten für Datenschutz und Informationsfreiheit an eine verantwortliche Stelle mit dem Inhalt,

> „Bewerberdaten, soweit diese per E-Mail an potentielle Arbeitgeber versendet werden, zu verschlüsseln oder derart zu pseudonymisieren, dass von den per E-Mail versandten Daten nicht auf die Identität der betroffenen Person geschlossen werden kann“

von dem dortigen Gericht formell nicht beanstandet worden, obwohl notwendige Folge der Anordnung selbstverständlich die Untersagung des unverschlüsselten E-Mail-Versands gewesen ist. Indem sich die angegriffene Entscheidung des Oberverwaltungsgerichts im hier vorliegenden Verfahren auf die „Deaktivierung“ als Untersagungsmaßnahme versteift, ignoriert diese, dass die Deaktivierung selbst Teil einer Beseitigungsmaßnahme ist. Beseitigt wird der Verstoß, der in der Nutzung einer unzureichenden Infrastruktur liegt. Nicht die Formulierung der Anordnung, sondern ihre objektiv verstandene Zielrichtung muss für die Auslegung hinsichtlich des Regelungsinhalts eines Verwaltungsaktes maßgeblich sein (vgl. Stelkens in Stelkens/Bonk/Sachs, Verwaltungsverfahrensgesetz 8. Auflage 2014, § 35, Rn. 71):

> „Dabei ist nicht an den Buchstaben zu haften, sondern auf den Willen der Behörde abzustellen, soweit dieser im Bescheid greifbar seinen Niederschlag gefunden hat.“
> (Stelkens in Stelkens/Bonk/Sachs, Verwaltungsverfahrensgesetz, 8. Auflage 2014, § 35, Rn. 76)

Es liefe auf eine Formalität hinaus, wenn statt einer „Deaktivierung“ die Beseitigung des rechtswidrigen Zustands „Nutzung“ angeordnet werden müsste. Das Ergebnis ist in beiden Fällen die gleiche Rechtsfolge, nämlich die Beendigung des Betriebs der Webseite auf Basis der Fanpage-Infrastruktur. Die Anordnung des Beklagten ist damit bei verständiger Würdigung ihres Inhalts als Maßnahme nach § 38 Abs. 5 S. 1 BDSG zu bewerten und als solche auch rechtmäßig erlassen worden.

Selbst wenn aber der Ansicht des Oberverwaltungsgerichts zu folgen sein sollte, dass die Aufforderung zur Deaktivierung als Untersagung im Sinne des § 38 Abs. 5 S. 2 BDSG zu werten ist, müsste ausnahmsweise auf die Stufenform des § 38 Abs. 5 BDSG verzichtet werden. Ein Verwaltungsakt, der Unmögliches anordnet, ist gemäß § 44 Abs. 2 Nr. 4 VwVfG nichtig. Der vom Oberverwaltungsgericht (US 20) vermisste

> „Raum, datenschutzrechtliche Verstöße abzustellen“

war zu keinem Zeitpunkt ansatzweise gegeben. Bereits im Vorverfahren war deutlich, und ist von der Beigeladenen ausdrücklich bestätigt worden, dass die Klägerin keinerlei Kontrolle über die Datenverarbeitung der Beigeladenen hat und keinerlei Möglichkeit besteht, korrigierend einzuwirken. So heißt es schon im Widerspruch (Anlage K 3 der Klagebegründung, dort S. 7) der Klägerin vom 06.12.2011:

> „Hier scheitert eine Auftragsdatenverarbeitung bereits daran, dass die Wirtschaftsakademie überhaupt keine Verfügungsgewalt über die durch Facebook erhobenen Daten hat. Die Wirtschaftsakademie hat auch nicht Möglichkeit, die Daten zur Verfügung gestellt zu bekommen.“

Trotzdem in einer Anordnung technische Änderungen an der zugrundeliegenden Infrastruktur zu verlangen, wäre mangels Vollziehbarkeit rechtlich unstatthaft gewesen. Die Aufforderung, die Webseite zu deaktivieren, war hingegen die einzig sinnvolle Regelungswirkung der Anordnung. Maßgebend ist hier auch allein die tatsächliche Ausführbarkeit durch die Klägerin, nicht durch die Beigeladene. Indem das Oberverwaltungsgericht meint, die Korrektur der Datenverarbeitungsprozesse sei jedenfalls für die Beigeladene nicht unmöglich im Sinne des § 44 Abs. 2 Nr. 4 VwVfG, überträgt es Aspekte der Auswahl des Adressaten in unzulässiger Weise in die Frage der Voraussetzungen für das Vorliegen einer Eingriffsgrundlage. Dies kann die Klägerin nicht entlasten.

Hierbei versäumt es das Oberverwaltungsgericht zudem, zu berücksichtigen, dass auch Art. 28 Abs. 3 der Richtlinie 95/46/EG ausschließlich darauf verweist, dass jede Kontrollstelle über

> “wirksame Einwirkungsbefugnisse, wie beispielsweise […] die Befugnis, die Sperrung, Löschung oder Vernichtung von Daten **oder** das vorläufige oder endgültige Verbot einer Verarbeitung anzuordnen, […]“
> (Hervorhebung RA)

verfügen. muss. Ein „abgestuftes Verfahren“, wie es die deutsche Vorschrift des § 38 Abs. 5 BDSG nach Lesart des Oberverwaltungsgerichts vorsieht, ist in der Richtlinie nicht vorgesehen. Stattdessen zählt die Richtlinie konkrete Maßnahmen, wie das Verbot einer Verarbeitung, auf hierarchisch gleicher Ebene auf. Dies spricht abermals dafür, dass in Beachtung der europarechtlichen Vorgaben bei dem Verhältnis zwischen Beseitigungsanordnung einerseits und Untersagungsanordnung andererseits die wirksame Beseitigung des Verstoßes im Vordergrund stehen muss. Diese fundamentale Bedeutung eines effektiven Schutzes der Betroffenen als prägender Gedanke der Befugnisse der nationalen Aufsichtsbehörden hat auch der EuGH stets hervorgehoben. Zuletzt betonte der EuGH im Urteil vom 6. Oktober 2015 (Case C-362/14, Maximillian Schrems v Data Protection Commissioner, Rz. 41):

> “The guarantee of the independence of national supervisory authorities is intended to ensure the **effectiveness** and reliability of the monitoring of compliance with the provisions concerning protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim.”

> “Die Garantie der Unabhängigkeit der nationalen Aufsichtsbehörden hat das Ziel, die **Effektivität** und Verlässlichkeit zu sichern, mit der die Einhaltung der Vorgaben bezüglich des Schutzes betroffener Personen überwacht wird. Diese Garantie muss im Lichte dieses Zieles interpretiert werden.“
> (Übersetzung und Hervorhebung Bekl.)

Angesichts der tatsächlichen Unmöglichkeit, die Verstöße auf Seiten der Beigeladenen zu beheben, stellt die Deaktivierung der Webseite auf Basis der Facebook-Infrastruktur die einzige effektive Maßnahme im Sinne des Art. 28 Abs. 3 95/46/EG sowie § 38 Abs. 5 BDSG dar und ist damit als rechtmäßig anzusehen.

Im Übrigen folgt aus den Ausführungen des Beklagten zur Grundrechtsbindung der Klägerin (S. 7 bis 13 der Revisionsbegründung) nicht, dass die Anordnung gegen eine öffentliche Stelle im Sinne des § 3 LDSG-SH gerichtet wurde. Die Klägerin ist eine nicht-öffentliche Stelle im Sinne des § 2 Abs. 4 S. 1 BDSG. Sie ist auch keine

öffentliche Stelle im Sinne des § 2 Abs. 4 S. 2 BDSG, weil sie keine Aufgaben des Bundes wahrnimmt (vgl. dazu Dammann, in: Simitis, BDSG, § 2, Rn. 45). Die Klägerin nimmt nichtsdestotrotz Bildungsaufgaben im Auftrag öffentlicher Stellen des Landes Schleswig-Holstein wahr und ist eine Schule in privater Trägerschaft nach § 1 Abs. 2 SchulG SH (insoweit zutreffend der Schriftsatz der Beigeladenen vom 12.05.2015, dort S. 44 und 45). Die daraus trotzdem folgende besondere Grundrechtsbindung wirkt sich bei der Bestimmung der Rechtspflichten der Kl. im Rahmen des Tatbestands des § 38 Abs. 5 BDSG aus (dazu direkt im Anschluss).

2.2. Zur Tatbestandlichkeit der Ermächtigungsgrundlage

Maßgebliche Voraussetzung für den Erlass einer Anordnung nach § 38 Abs. 5 S. 1 BDSG ist, dass die Aufsichtsbehörde Verstöße bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten oder technische oder organisatorische Mängel feststellt. Der Wortlaut des Tatbestands der Ermächtigungsgrundlage in § 38 Abs. 5 S. 1 BDSG grenzt den Anwendungsbereich dabei nicht auf verantwortliche Stellen im Sinne des § 3 Abs. 7 BDSG ein. Genauso wenig gibt Art. 28 Abs. 3 der Richtlinie 95/46/EG vor, dass sich der Tatbestand des Art. 28 Abs. 3 der Richtlinie 95/46/EG ausschließlich auf Verletzungen durch verantwortliche Stellen bezieht. Zwar spricht die Richtlinie 95/46/EG am Ende des Art. 28 Abs. 3 von der Befugnis

> „eine Verwarnung oder eine Ermahnung an den für die Verarbeitung **Verantwortlichen** zu richten“.
> (Hervorhebung RA)

Für die übrigen Befugnisse folgt daraus aber nicht zwingend die gleiche Voraussetzung, da die Aufzählung nicht kumulativ ist (Dammann, Dammann/Simitis, EG-Datenschutzrichtlinie, Art. 28, Erl. 10). Stattdessen ist in Art. 28 Abs. 3 95/46/EG primär von wirksamen Einwirkungsbefugnissen zur Behebung von Mängeln in Verarbeitungsverfahren die Rede. Als Voraussetzung verlangt die Ermächtigungsgrundlage damit primär das Vorliegen eines Verstoßes gegen die Vorgaben der auf Grund der Richtlinie 95/46/EG erlassenen Vorschriften. Die Frage, gegenüber wem ein Tätigkeitwerden der Aufsichtsbehörden zulässig ist, ist als Frage der Rechtsfolge von der Frage des Vorliegens des Tatbestandes des § 38 Abs. 5 BDSG zu trennen (dazu unten 2.3).

Ein den Tatbestand erfüllender Verstoß liegt hier vor. Die Klägerin nutzt für die Bereithaltung und Wartung ihres Webauftritts auf *https://www.facebook.com/wirtschaftsakademie* die Dienste der Beigeladenen. Deren Angebot kombiniert klassische Webhosting-Dienste, bei denen für fremde Inhalte eine Plattform bereitgestellt wird, mit einem eigenen Geschäftsmodell, durch das die über diese Webseiten laufenden Nutzungsdaten im eigenen Interesse monetarisiert werden. Hierzu schloss die Klägerin mit der beigeladenen Facebook Ireland Ltd. einen Vertrag über die Bereitstellung und Vorhaltung einer Webseite, durch dessen Umsetzung die dabei anfallenden Nutzungsdaten unter Verstoß gegen deutsches Datenschutzrecht verarbeitet werden. Dass zwischen Klägerin und Beigeladenen ein vertragliches Verhältnis besteht, räumt auch die Beigeladene in ihrem Schriftsatz vom 12.05.2015, dort S. 68, ein und führt aus:

> „Zwischen der Klägerin und der Beigeladenen besteht ein Nutzungsvertrag, der es der Klägerin ermöglicht, die Angebote der Beigeladenen auf Grundlage der Nutzungsbedingungen und Datenverwendungsrichtlinien zu nutzen“.

Diesen Sachverhalt ignoriert das Oberverwaltungsgericht (US 25), wenn es die rechtliche Schlussfolgerung zieht:

> „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.“

Klägerin und Beigeladene haben einen Vertrag über die Bereitstellung der als „Fanpage“ bezeichneten Webseite geschlossen. Notwendiger Inhalt dieses Vertrages ist auch die Verarbeitung der Daten der Besucher der Fanpage. Dem tritt auch die Klägerin nicht entgegen, sondern versucht stattdessen, ihr Verhältnis zur Beigeladenen mit dem jedes anderen Nutzers gleichzustellen, wenn sie ausführt (Schriftsatz vom 06.05.2015, S. 17):

> „Wie dargestellt ist Facebook nicht mehr und nicht weniger als eine Infrastruktur, auf der sich unterschiedliche Nutzer auf vollständig gleich geordneter Ebene und auf Grundlage identischer Nutzungsbedingungen begegnen. […] Die Beklagte nutzt die Infrastruktur.“

Diese Beschreibung wird nicht der tatsächlichen Interessen- und Sachlage gerecht, wie sie die Klägerin an anderer Stelle ihres Schriftsatzes vom 06.05.2015 (S. 23f) beschreibt:

> „Die Beklagte nutzt Facebook, weil Kunden und potenzielle Kunden der Beklagten genau diesen Kommunikationskanal nachfragen".

Dies zeigt, dass die Facebook-Fanpage der Klägerin auch in den Augen von Klägerin und Beigeladener kein privater Nutzeraccount in einem sozialen Netzwerk ist, sondern der Internetauftritt eines Unternehmens. Das wird bereits dadurch deutlich, dass private Seiten sich als Freunde hinzufügen können, während gegenüber Unternehmensseiten ein „Gefällt mir" ausgesprochen wird. Zudem sieht die Beigeladene eigene Nutzungsbedingungen für Facebook-Fanpages vor (letzte Änderung am 08.01.2015), die von den Nutzungsbedingungen für die Nutzer abweichen. Dort heißt es beispielsweise unter I. A.

> „Die Verwaltung einer Seite für eine Marke, ein Unternehmen (einen Ort oder eine Organisation) oder eine öffentliche Person darf ausschließlich von einem autorisierten Vertreter der jeweiligen Marke, des Unternehmens (Ortes bzw. der Organisation) oder der öffentlichen Person vorgenommen werden (eine „offizielle Seite")."

und unter I. C.

> „Auf einer Seite gepostete Inhalte sind öffentlich und für jeden sichtbar, der die Seite sehen kann."

Anlage B 5: Nutzungsbedingungen für Fanpages der Beigeladenen

Die Unternehmensseite der Klägerin, ihre Fanpage, ist damit kein normaler Nutzeraccount, sondern ein Internetauftritt, wie es ihn millionenfach im Internet gibt und wie ihn eine Vielzahl von Dienstleistern in ähnlicher Form anbietet. Faktisch unterscheidet sich das Angebot der Beigeladenen daher nicht von anderen Webseiten-Plattformen wie Wordpress, Tumblr, oder Squarespace. Allen diesen Angeboten ist zu eigen, dass der Seitenbetreiber sich die Wartungs- und Bereithaltungsarbeiten erspart, indem ein vorgefertigter Baukasten innerhalb einer bestehenden Infrastruktur genutzt wird.

Wo andere Anbieter nun beispielsweise Google Analytics vorinstalliert anbieten, ist in dem Angebot der Beigeladenen der Facebook Insight Dienst integriert und die Interaktion mit den Nutzeraccounts der Mitglieder des sozialen Netzwerks der Beigeladenen möglich. Das Oberverwaltungsgericht unterscheidet diesbezüglich unzureichend zwischen den privaten Nutzerkonten von Facebook-Mitgliedern und den in der Facebook-Infrastruktur gehosteten Seiten und kommt schon von daher durch Zugrundelegung eines unrichtigen Sachverhalts auch zu unrichtigen rechtlichen Schlüssen.

Zur grundsätzlichen Vergleichbarkeit einer Facebook-Fanpage mit einem Internetauftritt hat die Rechtsprechung dabei bereits vielerorts unter dem Aspekt der Impressumspflicht Stellung bezogen. Maßgeblich hat das LG Köln im Urteil vom 28. Dezember 2010 (Az. 28 O 402/10) über eine Blogging-Plattform entschieden. Danach stellte der dortige Anbieter eine

> „technische Plattform in Form von Speicherplatz und technischer Infrastruktur für C1 auf ihren Servern in den Vereinigten Staaten bereit. Diese können sich einen Account anlegen und unter Zuhilfenahme der technischen Infrastruktur und des Speicherplatzes auf der Domain der Verfügungsbeklagten www.C1.com Blogs veröffentlichen. Die Accounts werden mit der Angabe einer Emailadresse von den Nutzern/Bloggern verifiziert. Die Inhalte der Blogs überprüft die Verfügungsbeklagte nicht. Die Domain und den Bloggerdienst nutzt die Verfügungsbeklagte kommerziell. Sie ist Administrator der Internetseite C2.com.“

Mit Verweis auf die identische tatsächliche Situation wird in der Rechtsprechung seitdem einhellig auch von Betreibern einer Facebook-Seite etwa die Erfüllung der Impressumspflicht eingefordert (vgl. etwa das LG Aschaffenburg mit Urteil vom 19.8.2011 [Az. 2 HK O 54/11] unter Verweis auf das zitierte Urteil des LG Köln). Die Klägerin betreibt ihre Internetseite in gleicher Weise unter Rückgriff auf die Dienste der Beigeladenen.

Dem tritt die Klägerin nicht entgegen, versucht aber trotzdem zu betonen, dass zwischen einem Internetauftritt unter Eigenregie und der Nutzung einer Fanpage ein Unterschied bestehe. Zu diesem Zweck verweist sie in ihrer Stellungnahme vom 06.05.2015 (S. 19) darauf, dass sie lediglich einen Kausalbeitrag zur Datenverarbeitung der Beigeladenen leiste und eine daraus abzuleitende Verantwortung

„dem aus gutem Grund gesetzgeberisch fein gegliederten datenschutzrechtlichen Verantwortungskonstrukt“

nicht gerecht würde. Die Klägerin betont immer wieder, dass sie auf die einzelnen technischen Details der Infrastruktur, die sie für ihre Fanpage nutzt, keinerlei Einfluss hat. Das wird durch den Beklagten auch gar nicht bestritten. Dies führt aber nicht zu der mit diesem Argumentationsstrang bezweckten Entlastung der Klägerin aus ihrer datenschutzrechtlichen Verantwortung. Ansatzpunkt für die angegriffene Anordnung des Beklagten ist nicht eine ohne Beteiligung der Beigeladenen vorgenommene Verarbeitung von Nutzerdaten, sondern die Datenverarbeitung im Rahmen der eigenen Webseite, für deren Umsetzung auf die Infrastruktur der Beigeladenen zurückgegriffen wird. Diese Infrastruktur enthält datenschutzrechtlich zu beanstandende Elemente. Die einer eigenen Zweck- und Mittelentscheidung folgende Inanspruchnahme der insofern mangelhaften Infrastruktur stellt damit einen Mangel im Betrieb der Internetseite der Klägerin dar.

Zu den Mängeln dieser von der Klägerin genutzten Infrastruktur war in den Vorinstanzen ausführlich vorgetragen worden. Insoweit wird auf die zuletzt in der Revisionsbegründung gemachten Ausführungen (S. 55f) verwiesen. Diese betreffen nicht nur, aber auch die fehlende Umsetzung der Vorgaben des TMG bezüglich der Nutzbarkeit unter Verwendung von Pseudonymen (§ 13 Abs. 6 TMG), der Widerspruchsmöglichkeit gegen Nutzerprofile (§ 15 Abs. 3 S. 1 TMG) und der unzulässigen Verbindung von pseudonymen Nutzerprofilen mit den Trägern des Pseudonym (§ 15 Abs. 3 S. 3 TMG). Zudem verarbeitet die Beigeladene bei dem Betrieb der Facebook-Infrastruktur personenbezogene Daten auch solcher Fanpage-Besucher, die nicht Mitglied im sozialen Netzwerk sind, sondern lediglich die Fanpage der Klägerin als Nicht-Mitglied besuchen (dazu direkt im Anschluss unter 2.2.1).

2.2.1. Urteil des Dutch-Speaking Court of First Instance Brussels vom 09.11.2015

Über die IP-Adresse und den datr-Cookie erkennt die Beigeladene Details über das Surfverhalten dieser Nicht-Mitglieder, ohne dafür eine Einwilligung oder eine Rechtsgrundlage zu haben. Dazu wurde bereits ausführlich in der Revisionsbegründung (S.57ff) vorgetragen. Die Auffassung des Bekl. wird nunmehr gestützt durch das Urteil des Brüsseler Instanzgerichts vom 09.11.2015 (Fallnummer 15/57/C), welches im französischen Original

Anlage B 6**:** Urteil des Tribunal de Première Instance Néerlandophone de Bruxelles vom 09.11.2015, in französischer Sprache

und in der englischen Übersetzung durch die Commission de la protection de la vie privée beigefügt ist.

Anlage B 7: Urteil des Dutch-Speaking Court of First Instance Brussels vom 09.11.2015, in englischer Sprache

Im dortigen Verfahren bestätigte das Gericht, dass der datr-Cookie der Beigeladenen personenbezogene Daten enthalte und es hierfür und zu dessen Verarbeitung an einer Rechtsgrundlage fehle. Das Brüsseler Instanzgericht führt zum Personenbezug des datr-Cookie aus (S. 22f):

> „The datr cookie which Facebook places on the computer of an Internet user and by means of which it receives information, uniquely identifies the Internet browser of an Internet user. The cookie contains a "unique identifier". Facebook also receives additional information enabling it to directly or indirectly identify individuals, such as the IP address of the Internet user's computer.
>
> Both the Court of Justice of the EU and the "Article 29" Data Protection Working Party have already confirmed explicitly that IP addresses are "personal data" *(see among Court of Justice Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) of 24 November 2011 C-70/10, marginal no. 51 i.f. "Those addresses are protected personal data because they allow those users to be precisely identified.").*
>
> Since the defendants state themselves that the datr cookie is used, among others to perform a certain type of access control and therefore partially to determine who will be granted or denied access to a Facebook service, the datr cookie as such must also be considered as personal data."

Deutsche Übersetzung:

> „Der datr-Cookie, den Facebook auf dem Computer eines Internetnutzers platziert und durch den es Informationen erhält, identifiziert den Internet Browser eines Internetnutzers eindeutig. Dieser Cookie enthält eindeutige Identifikatoren. Facebook erhält zudem weitere Informationen, die es ermöglichen, Individuen

direkt oder indirekt zu identifizieren, wie etwa die IP-Adresse des Computers des Internetnutzers.

Sowohl der Gerichtshof der europäischen Union als auch die Art. 29 Datenschutzgruppe haben bereits ausdrücklich bestätigt, dass es sich bei IP-Adressen um „personenbezogene Daten“ handelt *(siehe unter vielen das Urteil des Gerichtshofs der europäischen Union, Scarlet Extended SA gegen Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) vom 24. November 2011C-70/10, Randziffer 51: „Bei diesen Adressen handelt es sich um geschützte personenbezogene Daten, da sie die genaue Identifizierung der Nutzer ermöglichen“).*

Da die Beklagte selbst erklärt, der datr-Cookie werde benutzt, um, unter anderem, eine gewisse Form der Zugangskontrolle durchzuführen und dabei teilweise zu entscheiden, wem Zugang zu den Facebook-Diensten gewährt wird und wem nicht, muss dieser Cookie auch als personenbezogenes Datum gewertet werden.“

(Englische Übersetzung des französischen Urteilstextes durch die Commission de la protection de la vie privée, deutsche Übersetzung durch den Bekl.)

Zur fehlenden rechtlichen Legitimation, insbesondere zur fehlenden Einwilligung führt das Brüsseler Gericht aus (S. 24 f):

„By clicking on the hyperlink behind the words *"our cookie policy"* visitors are brought to a page *"Cookies, Pixels and Similar Technologies",* which provides quite some explanation about cookies, although the datr cookie as such is not mentioned there.

Apparently the datr cookie is not placed at that moment yet, but it is placed in case of further clicks of the non-registered user on this page, for instance on the hyperlinks *"Facebook services"* or *"our Statement of Rights and Responsibilities".*

Likewise the datr cookie is apparently not placed when a non-registered user clicks on a Facebook social plug in, consciously or not, from a web page outside the Facebook domain. But if the user then clicks "cancel" to close the social plug-in, apparently the cookie is indeed placed.

The court is of the opinion that Facebook cannot consider these actions as granting informed consent, because in the first case the user is still gathering information, and further examining the information cannot be considered as use of the Facebook services. In the second case the same non-registered user, precisely by closing the social plug-in, indicates that he does not wish to use the service offered.

Likewise the court is of the opinion that Facebook does not have informed and unambiguous consent to read a previously placed datr cookie from a non-registered user's browser. After all, pursuant to Article 129 of the ECA the controller must have consent to store information as well as gain access to information which is already stored in a user's final equipment."

Deutsche Übersetzung:

„Durch Klicken auf den Hyperlink hinter den Wörtern *„our cookie policy"* gelangen Besucher zu der Seite *„Cookies, Pixels and Similar Technologies"*, die viele Erklärungen über Cookies enthält, wobei der datr-Cookie als solcher nicht erwähnt wird.

Offenbar wird der datr-Cookie in diesem Moment noch nicht platziert, aber er wird in dem Fall platziert, dass der nicht-registrierte Nutzer weitere Inhalte auf dieser Seite anklickt, etwa die Hyperlinks *„Facebook services"* oder „*our Statment of Rights and Responsibilities".*

Ebenso wird der datr-Cookie offenbar nicht platziert, wenn ein nicht-registrierter Nutzer auf ein Facebook-Social-Plugin auf einer Webseite außerhalb von Facebook klickt, bewusst oder unbewusst. Klickt der Nutzer dann aber auf „Cancel", um das Social-Plugin zu schließen, wird der Cookie offenbar tatsächlich gesetzt.

Das Gericht ist der Ansicht, dass Facebook derartige Handlungen nicht als informierte Einwilligung behandeln kann, weil im ersten Fall der Nutzer noch dabei ist, sich Informationen zu beschaffen und das bloße Informieren über die Dienste von Facebook nicht bereits als Nutzung dieser Dienste gewertet werden kann. Im zweiten Fall zeigt der nicht-registrierte Nutzer gerade durch Schließen

des Social Plugins an, dass er nicht wünscht, die angebotenen Dienste zu nutzen.

Ebenso ist das Gericht der Ansicht, dass Facebook keine informierte und ausdrückliche Einwilligung zum Lesen der bereits platzierten datr-Cookies aus dem Browser von nicht registrierten Nutzern hat. Schließlich muss die verantwortliche Stelle sowohl für die Speicherung als auch für den Zugriff auf Informationen, die bereits auf dem Gerät des Nutzers gespeichert sind, eine Einwilligung haben."

(Englische Übersetzung des französischen Urteilstextes durch die Commission de la protection de la vie privée, deutsche Übersetzung durch den Bekl.)

Der rechtlichen Wertung dieses Sachverhalts durch das Brüsseler Instanzengericht haben sich die Aufsichtsbehörden der Niederlande, Frankreichs, Spaniens sowie Hamburgs und Belgiens in einer gemeinsamen Erklärung vom 04.12.2015

Anlage B 8**:** Common Statement by the Contact Group of the Date Protection Authorities of The Netherlands, France, Spain, Hamburg and Belgium vom 04.12.2015

angeschlossen, da die dem belgischen Urteil zugrundeliegenden rechtlichen Vorgaben europaweit gelten.

Dass auf das Angebot der Beigeladenen deutsches Datenschutzrecht anwendbar ist, wurde bereits mit Verweis auf das Urteil des EuGH vom 13.5.2014 (C-131/12 - Google Spain) in der Revisionsbegründung (S. 56) dargelegt. Diese Auffassung wurde jüngst durch das Urteil des EuGH vom 01.10.2015 (C-230/14 – Weltimmo – abgedruckt in DuD 2015, Heft 12, S.830 (832)) bestätigt. Der EuGH führt dort in Randziffer 41 aus:

„Art. 4 Abs. 1 Buchst. a der Richtlinie 95/46 ist dahin auszulegen, dass er die Anwendung des Datenschutzrechts eines anderen Mitgliedstaats als dem, in dem der für die Datenverarbeitung Verantwortliche eingetragen ist, erlaubt, soweit dieser mittels einer festen Einrichtung im Hoheitsgebiet dieses Mitgliedstaats eine effektive und tatsächliche Tätigkeit ausübt, in deren Rahmen diese Verarbeitung ausgeführt wird, selbst wenn die Tätigkeit nur geringfügig ist."

Der EuGH bestätigt damit den weiten Niederlassungsbegriff. Zweifel daran, dass die im Rahmen der Facebook Germany GmbH in Hamburg ausgeübte Tätigkeit dazu führt, dass die Infrastruktur der Beigeladenen der Anwendung des deutschen Datenschutzrechts unterliegt, sollten damit in Übereinstimmung mit der Rechtsprechung des EuGH obsolet sein.

2.2.2. Google-Spain-Entscheidung

In diesem Zusammenhang ist nochmals die von der Beigeladenen vertretene Auffassung, die soeben bereits angesprochene Google-Spain-Entscheidung sei ohne Bedeutung für den vorliegenden Rechtsstreit (S. 81), zurückzuweisen.

Der Beigeladenen ist nur insoweit zuzustimmen, als dem hier vorliegenden Rechtsstreit kein unmittelbar vergleichbarer Sachverhalt zugrunde liegt. Hingegen hat die Google-Spain-Entscheidung mit ihren grundsätzlichen Aussagen zu Fragen der Verantwortlichkeit, der Geltung deutschen Rechts bei Angeboten ausländischer Anbieter und der Auslegung des einfachgesetzlichen Rechts grundsätzliche Bedeutung für den vorliegenden Rechtsstreit.

So ist durch die Google-Spain-Entscheidung klargestellt, dass deutsche Betreiber von Fanpages wie die Kl. sich nicht mehr darauf berufen können, dass die Verarbeitung von Facebook nach dem Recht anderer Staaten möglicherweise rechtmäßig sein könnte. Mit dem EuGH ist davon auszugehen, dass Anbieter von Kommunikationsplattformen nach den in der Entscheidung verwandten Kriterien ohne Zweifel das deutsche Datenschutzrecht, also BDSG und TMG, zu beachten haben.

2.2.3. Schrems-Urteil des EuGH

Neben den vorstehend zusammengefassten datenschutzrechtlichen Mängeln der Facebook-Infrastruktur ist als weiterer essentieller Mangel die Verarbeitung der Daten in einem Drittland ohne angemessenes Datenschutzniveau festzustellen. In dem am 06.10.2015 ergangenen Urteil in Sachen Maximillian Schrems gegen Data Protection Commissioner hat der EuGH entschieden, dass die Safe-Harbor-Entscheidung der Kommission

> „gegen die in Art. 25 Abs. 6 der Richtlinie 95/46 im Licht der Charta festgelegten Anforderungen verstößt und aus diesem Grund ungültig ist“. (RN 98)

Die Daten der Besucher der Fanpage der Klägerin wurden und werden auf Basis von unwirksamen rechtlichen Grundlagen von dem von der Klägerin gewählten Infrastrukturdienstleister in die USA übermittelt. Diese rechtliche Grundlage, die Safe-Harbor-Grundsätze, sind, wie das Urteil des EuGH (RN 94) bestätigt, unzureichend, um ein angemessenes Schutzniveau für die Besucher der Website der Klägerin herzustellen, insbesondere weil

> „eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des durch Art. 7 der Charta garantierten Grundrechts auf Achtung des Privatlebens“

verletzt. Einen derartigen Eingriff in den Kernbereich eines Grundrechts können die Safe-Harbor-Grundsätze gemäß dem Urteil des EuGH (RN 86) nicht rechtfertigen, weil darin

> „den „Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen“ Vorrang vor den Grundsätzen des „sicheren Hafens“ eingeräumt“

wird. Die Unwirksamkeit des Safe-Harbor-Entscheidung besteht nicht erst mit dem Entscheidungsdatum des Urteils vom 06.10.2015, sondern das Urteil hat die Ungültigkeit der Safe-Harbour-Entscheidung 2000/520 der Kommission vom 26.07.2000 ohne zeitliche Beschränkung und damit von Anfang an festgestellt. Dies liegt auf der Linie der bisherigen Rechtsprechung des EuGH. Im Urteil vom 26. April 1994 (C-228/92, in Sachen Roquette Freres Sa gegen Hauptzollamt Geldern, RN 17) führt das Gericht aus:

> „Ein Urteil des Gerichtshofes, mit dem im Vorabentscheidungsverfahren eine Gemeinschaftshandlung für ungültig erklärt wird, besitzt grundsätzlich ebenso wie ein Nichtigkeitsurteil Rückwirkung.“

Damit fehlte zum Zeitpunkt des Erlasses der streitgegenständlichen Anordnung des Beklagten eine zureichende Rechtsgrundlage für die Datenübermittlung der Beigeladenen an die Facebook Inc. in den USA. Dem Nutzungsverhältnis zwischen

Klägerin und Beigeladenen, das die Vorhaltung und Wartung der Fanpage der Klägerin begründet, liegt damit seit Freischaltung der Webseite der Klägerin durch die Beigeladene zudem ein weiterer wesentlicher Mangel der Infrastruktur zugrunde.

Im Ergebnis nutzt die Klägerin das Angebot eines Dienstleisters, der nicht die nötige Gewähr dafür bietet, dass die beim Betrieb der Webseite www.facebook.com/wirtschaftsakademie verarbeiteten Daten dem deutschen Datenschutzrecht entsprechend verarbeitet werden. Dies stellt einen Mangel im Sinne des § 38 Abs. 5 S. 1 BDSG des Webauftritts der Klägerin dar. Damit waren und sind die Voraussetzungen des Eingriffstatbestandes, auf den sich der Beklagte stützt, erfüllt.

Dies gilt insbesondere unter Berücksichtigung der in der Revisionsbegründung (S. 7ff) dargestellten verstärkten Grundrechtsbindung, der die Klägerin unterliegt. Als private Schulträgerin ist sie in noch stärkerem Maße zur Wahl datenschutzrechtlich unbedenklicher Infrastrukturen verpflichtet, auf deren Basis sie sich im Internet präsentieren will, als es auch Fanpage-Betreiber ohne jede öffentlich-rechtliche Bindung in Beachtung der Datenschutzgesetze ohnehin sind. All diese Zusammenhänge hat das angegriffene Urteil rechtsfehlerhaft außer Acht gelassen.

2.3. Zur Rechtsfolge der Ermächtigungsgrundlage

Als Rechtsfolge sieht § 38 Abs. 5 S. 1 BDSG vor, dass die zuständige Aufsichtsbehörde Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel anordnet. Der Beklagte hat die Deaktivierung der auf Basis der Infrastruktur der Beigeladenen errichteten Webseite angeordnet.

Diese Anordnung richtete sich mit der Klägerin als Adressatin auch an eine ermessensfehlerfrei ausgewählte Störerin, weil die Klägerin als Betreiberin der Webseite verantwortlich für die datenschutzrechtliche Rechtmäßigkeit ihres Webauftritts ist. Eine solche Verantwortlichkeit lehnte das Oberverwaltungsgericht sowohl unter dem Gesichtspunkt der eigenen Datenverarbeitung als auch unter dem Gesichtspunkt der Verarbeitung durch Dritte ab, wenn es (US 22) ausführt, die Klägerin erhebe und verarbeite

> „keine personenbezogenen Daten der Besucher der Fanpage für sich selbst“.

und andererseits (US 25), die Klägerin sei

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

Das Oberverwaltungsgericht macht für eine selbstständige Datenverarbeitung in unzulässiger Weise zur Voraussetzung einer Verantwortlichkeit der Klägerin, dass diese mit den Daten ihrer Nutzer in Berührung komme oder diese eigenständig übermittle. Beides scheide nach Ansicht des angegriffenen Urteils insbesondere deshalb aus, weil die Klägerin als Fanpagebetreiberin weder über das „Warum“ der Datenverarbeitung entscheide noch über die eingesetzten Mittel:

> „Die Zwecke sind zu unterscheiden. Der Fanpagebetreiber entscheidet nicht über den Zweck, das heißt das „Warum“ der Verarbeitung von personenbezogenen Daten zusammen mit Facebook, vielmehr bestimmt Facebook diesen Zweck allein.“ (US 22)

> „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.“ (US 23)

Dabei lässt das Oberverwaltungsgericht vollständig außer Acht die dem Verhältnis von Beigeladener und Klägerin zugrunde liegende und bewusst eingesetzte technische Arbeitsteilung, die für den Betrieb der Fanpage der Klägerin innerhalb der Infrastruktur der Beigeladenen maßgeblich ist. Die Fanpage ist eine Webseite, für deren Betrieb sich die Klägerin Dienstleistungen der Beigeladenen zu Nutze macht, und deren Betrieb durch die Beigeladene sowohl als Dienstleistung gegenüber der Klägerin als auch zu eigenen Geschäftsinteressen erfolgt. Wie jede eigenverantwortlich betriebene Internetseite ist die Klägerin nach § 12 Abs. 3 TMG und § 3 Abs. 7 BDSG für die im Rahmen des Webauftritts verarbeiteten Daten verantwortlich. Dies betrifft nach der klaren Definition des § 2 S. 1 Nr. 1 TMG auch eine Anbieterin,

> „die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt“.

Dies ist hinsichtlich der Impressumspflicht auch völlig unstrittig. Im Urteil des Landgerichts Hamburg vom 19. August 2010 (Az. 327 O 332/10) entschied das dortige Gericht deshalb:

> „Soweit die Antragsgegnerin vorgetragen hat, am 23.4.2010 sei nicht sie selbst, sondern vielmehr die Firma … Inc. in den USA für die Homepage verantwortlich gewesen, vermag dies ein abweichendes Ergebnis ebenfalls nicht zu begründen.
>
> Ausweislich der Anlagen handelt es sich hierbei um den Internetauftritt der Antragsgegnerin. Hierfür spricht ihre blickfangmäßig herausgestellte Firmenangabe »… GmbH« sowie der in deutscher Sprache gehaltene Inhalt. Nicht handelt es sich bei dem in Rede stehenden Online-Auftritt um eine »eu«-Domain – die Antragsgegnerin wiederum ist ausweislich der Anlage gerade auch für Europa zuständig, was die Annahme einer Diensteanbietereigenschaft der Antragsgegnerin i. S. v. TMG § 2 Nr. 1 TMG begründen dürfte.
>
> Soweit die Antragsgegnerin zum streitgegenständlichen Zeitpunkt die Gestaltung ihrer Internetpräsenz möglicherweise auf die Firma … Inc., als Beauftragte, übertragen hatte, entbindet sie dies nicht von der ihr – als Diensteanbieter (s. o.) – obliegenden Impressumspflicht (TMG § 5 Abs. l TMG). Das Verhalten ihrer Beauftragten muss sich die Antragsgegnerin gemäß UWG § 8 Abs. 2 UWG zurechnen lassen.“

Genauso kann es auch datenschutzrechtlich keine Rolle spielen, wer für die Klägerin die Wartung der Webseite übernimmt oder wer die technische Infrastruktur vorhält. Entscheidend ist, dass die Klägerin sich bezüglich der Erstellung der Webseite dafür entschied, die von der Beigeladenen angebotenen Dienste für die eigenen Kommunikationszwecke zu nutzen und als Mittel gerade die Infrastruktur der Beigeladenen wählte. Damit liegt die notwendige Entscheidung über Zwecke und Mittel im Sinne des § 3 Abs. 7 BDSG bzw. im Sinne des Art. 2 d) der RL 95/46/EG vor.
Dass die im Hintergrund ablaufenden Verarbeitungsprozesse für die Klägerin uninteressant sind oder nicht jeder Aspekt des Angebots der Beigeladenen gleichermaßen relevant für die Wahl des Mittels „Fanpage“ war, ist dabei unerheblich, weil

> „die Verantwortlichkeit einer Person oder einer Stelle nicht davon abhängt, ob sie Daten selbst speichert (und verarbeitet) oder ob sie sich dazu eines anderen, z.B. eines Service-Rechenzentrums oder eines Datenerfassungsbüros, bedient.“ (Dammann, Simitis, Bundesdatenschutzgesetz, 8. Auflage, § 38, Rn 227).

Eine solche Auslagerung der technischen Durchführung wird rechtlich stattdessen durch die Regelungen der Auftragsdatenverarbeitung abgebildet. Es ist der Auftragsdatenverarbeitung immanent, dass der Auftraggeber sich der eigentlichen Arbeitsvorgänge vollständig oder bezüglich abtrennbarer Teile entledigt und sich auf den Akt der Auftragserteilung beschränkt. Damit entledigt sich der Auftraggeber seiner Kontrolle über die zugrundeliegenden Arbeitsvorgänge. Als Korrektiv für diesen Kontrollverlust verlangt das deutsche Datenschutzrecht vertragliche und tatsächliche Kompensationen in Form vertraglich festgelegter Weisungsbefugnisse und schriftlicher Auftragsdatenverarbeitungsverträge gemäß § 11 Abs. 2 BDSG. Das Fehlen dieser Kompensationen für den mit der Auftragserteilung erlittenen Kontrollverlust ist gemäß § 43 Abs. 1 Nr. 2a BDSG ein eigenständig zu ahndender Verstoß. Vor diesem Hintergrund wird die für sich plausibel klingende Äußerung des Oberverwaltungsgerichts (US 25)

> „Eine Auftragsdatenverarbeitung ohne Auftrag gibt es nicht.“

der Systematik der Auftragsdatenverarbeitung nicht gerecht.

Das Fehlen eines ausreichenden und schriftlichen Auftragsdatenverarbeitungsvertrags kann kein Grund für eine Verneinung der Verantwortlichkeit des Auftraggebers sein, sondern ist ganz im Gegenteil ein selbstständiger Verstoß im datenschutzrechtlichen Sinne. Die fehlenden Festlegungen bezüglich der nötigen Weisungs- und Kontrollrechte zwischen Klägerin und Beigeladenen hätte das Oberverwaltungsgericht vielmehr zum Anlass nehmen müssen, den Nutzungsvertrag zwischen der Klägerin und der Beigeladenen konkret zu prüfen. Das Oberverwaltungsgericht meint stattdessen, aus der faktischen Unwilligkeit der Beigeladenen zur Duldung von Kontrollen als eines gesetzlich vorgesehenen Bestandteiles der Auftragsdatenverarbeitung darauf schließen zu können, dass auch rechtlich keine Auftragsdatenverarbeitung vorliegen könne. Es führt dazu aus (US 25):

> „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 wiederspiegeln, 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."

Das Oberverwaltungsgericht überbetont damit die Indizwirkung der faktischen Machtverhältnisse zwischen Klägerin und Beigeladener, indem es von der beschränkten Gestaltungsmöglichkeit eines Vertragspartners auf die rechtliche Nichtexistenz eines Auftragsdatenverarbeitungsverhältnisses schließt. Die Auffassung des Oberverwaltungsgerichts führte in der Konsequenz zu dem Ergebnis, dass ein Auftragnehmer durch faktische Weigerung der Umsetzung eines Vertrages ein bestehendes Auftragsdatenverarbeitungsverhältnis beseitigt oder, wie im vorliegenden Fall, auf Grund der durch seine Marktmacht ermöglichten Vorgabe der Auftragsinhalte und deren Modalitäten erst gar kein Auftragsdatenverarbeitungsverhältnis entstehen lässt. Das hätte zu Ende gedacht zum einen die Folge, dass die zuvor verantwortliche Stelle ihrer datenschutzrechtlichen Verantwortlichkeit entledigt wäre und sogar durch bewusste Auswahl eines unzuverlässigen Auftragnehmers sich der Verantwortlichkeit entziehen könnte, die andererseits aus der Beauftragung folgen würde. Und das hätte zu Ende gedacht zum anderen die Folge, dass ein Auftragsverhältnis deshalb erst gar nicht entsteht, weil der andere Vertragspartner sich von vorne herein auf keinerlei Vertragsverhandlungen einlässt und vor der Wahl steht, die Leistungen des Auftragnehmers nicht in Anspruch zu nehmen und auf sie zu verzichten, oder wegen des erwarteten eigenen Vorteils die gesetzten Bedingungen akzeptiert, ob nun gerne oder nur notgedrungen.

Dem gleichen Fehlschluss erliegt auch Petri (Datenschutzrechtliche Verantwortlichkeit im Internet, ZD 2015, S. 103 ff), der ebenfalls unter Bezugnahme auf die Rechtsprechung des Berufungsgerichts eine Verantwortlichkeit aufgrund eines Auftragsdatenverarbeitungsverhältnisses ablehnt und später (Auftragsdatenverarbeitung - heute und morgen - Reformüberlegungen zur Neuordnung des Datenschutzrechts, ZD 2015, S. 308 ff.) ausdrücklich wiederholt, unter Bestätigung des Urteils des OVG ausführt:

> „Wird der Vertrag nicht gelebt […] und kann der Auftraggeber keine Kontrolle ausüben, liegt keine Auftragsdatenverarbeitung vor“.

und auf S. 308 des gleichen Aufsatzes hinzufügt:

> „Übt der Auftraggeber seine Kontrolle tatsächlich nicht aus, liegt auch kein Auftragsverhältnis i.S.d. § 11 BDSG vor“.

Dabei übersieht Petri in beiden Fällen aber genauso wie das in Bezug genommene Oberverwaltungsgericht, dass ein Auftragsdatenverarbeiter, der sich faktisch jeder Weisung und Kontrolle durch den Vertragspartner verweigert, lediglich die Fehlerhaftigkeit der Auftragsdatenverarbeitung verursacht und dies zu Sanktionen für den Auftraggeber führt, der den Auftrag nicht in der vorgegebenen Weise erteilt und durchgeführt hat (Petri in: Simitis, Bundesdatenschutzgesetz, 8. Auflage, § 11, Rn. 64). In der Literatur besteht deshalb auch kein Zweifel daran, dass die Beauftragung eines ungeeigneten Auftragnehmers ein nach § 38 Abs. 5 BDSG zu ahndender Verstoß ist. So weist Petri (in: Simitis, Bundesdatenschutzgesetz, § 38, Rn. 73) mit Verweis auf Herb (in: Computer und Recht 1992, S. 113) selbst zu Recht darauf hin, dass die

> „Auftragsdatenverarbeitung mit einem bestimmten unzuverlässigen Vertragspartner“

untersagt werden kann. Dass sowohl Petri als auch Herb eine darauf gerichtete Anordnung als Anwendungsfall einer Untersagungsverfügung nach § 38 Abs. 5 S. 2 BDSG und nicht als Beseitigungsanordnung nach § 38 Abs. 5 S. 1 BDSG einordnen, begegnet den gleichen Bedenken wie unter 2.1 formuliert. Entscheidend ist hinsichtlich der Voraussetzungen des § 38 Abs. 5 BDSG einzig, dass die Nutzung eines Angebots von einem unzuverlässigen Dienstleister ein Datenschutzverstoß ist, dem der Beklagte im Anordnungswege begegnen musste.

2.3.1 Vergleichbarkeit mit Google Analytics

In diesem Zusammenhang verkennt das Oberverwaltungsgericht auch die tatsächlich bestehende rechtliche Vergleichbarkeit mit Reichweitenanalyse-Werkzeugen wie

Google Analytics. Die Klägerin mag kein eigenes Interesse an den weiteren Datenverarbeitungen der Beigeladenen haben, die diese im eigenen Interesse auf die durch die Fanpage gewonnenen Nutzerdaten anwendet. Das angegriffene Urteil führt dazu aus (US 24):

> „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“

Dem Oberverwaltungsgericht ist dabei insoweit zuzustimmen, dass die Klägerin den Reichweiten-Analysedienst „Facebook Insights“ nicht selbst in die eigene Fanpage integriert hat. Dies ist gemäß der soeben dargestellten Rechtslage für die Verantwortlichkeit aber auch nicht entscheidend. Entscheidend ist, dass die Klägerin die Dienste der Beigeladenen beauftragt hat und in Anspruch nimmt und zu diesen gehört neben der generellen Inanspruchnahme der von Facebook zur Verfügung gestellten Kommunikationsstruktur auch die Facebook-Insights Funktion.

Es kann nun keinen Unterschied machen, ob die Klägerin die Webseite in eigener Zugriffssphäre selbst vorhält und sich dabei bewusst für einen beliebigen Dienst zur Reichweitenanalyse entscheidet oder sich dafür entscheidet, diese technische Umsetzung durch einen Dienstleister vornehmen zu lassen.

Während die Einbindung von Diensten wie Google Analytics nach ganz gängiger Praxis im Rahmen einer Auftragsdatenverarbeitung geschieht (vgl. die Hinweise des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit zum beanstandungsfreien Betrieb von Google Analytics vom 15.09.2011),

Anlage B 9: Hinweise des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit zum beanstandungsfreien Betrieb von Google Analytics vom 15.09.2011

kann dies im vorliegenden Fall nicht deshalb anders beurteilt werden, weil sich die Klägerin zusammen mit der Inanspruchnahme der Kommunikationsstruktur der

Beigeladenen zugleich für die Inanspruchnahme des Facebook-Insights-Dienstes entscheidet, der in die von ihr gewählte Infrastruktur der Beigeladenen bereits implementiert ist. Es läge vielmehr an der Klägerin, etwaige Bedenken gegen die für die Insights-Funktion notwendigen Datenverarbeitungsvorgänge bei der Beigeladenen im Rahmen des Auftragsverhältnisses zur Sprache zu bringen. Dass dies wegen der bisherigen Ablehnung jeglicher Einflussnahme durch die Beigeladene bislang zunächst wenig aussichtsreich scheint, führt – abermals – nicht zur Entlassung aus der Verantwortlichkeit, sondern begründet einen eigenen Verstoß aufgrund unzureichender Erteilung und Durchführung des Auftrags.

Dass sich die Fanpage innerhalb der Facebook-Infrastruktur befindet, kann die Klägerin dabei genauso wenig aus ihrer datenschutzrechtlichen Verantwortlichkeit entlassen, wie die Nutzung jeder anderen Hosting-Plattform. Das Angebot an Dienstleistern, die über einfach bedienbare Oberflächen das intuitive Erstellen von Webseiten nach dem Baukastenprinzip ermöglichen, ist nahezu unüberschaubar. All diese Angebote gleichen sich dabei darin, dass der für die Inhalte Verantwortliche sich die technische Einrichtung, das Mieten eines Webservers und das Pflegen einer eigenen Infrastruktur durch Nutzung derartiger Angebote erspart und sich auf die Veröffentlichung von Inhalten konzentrieren kann. Dass diese Seiten neben der Möglichkeit des öffentlichen Abrufs auch die tiefergehende Interaktion im Sinne einer sozialen Plattform vorsehen, ist ebenfalls weder auf die Facebook-Infrastruktur noch auf sonstige Plattformen beschränkt.

Indem sich die Klägerin dazu entschied, neben ihrer primären Webpräsenz unter www.wak-sh.de/ auch unter www.facebook.com/wirtschaftsakademie eine Webseite zu unterhalten, hat sie für beide Webseiten die gleiche Verantwortlichkeit bezüglich der Einhaltung der maßgeblichen Vorschriften. Die Klägerin ist sowohl für die Datenverarbeitung unter www.wak-sh.de/ als auch für diejenige unter www.facebook.com/wirtschaftsakademie verantwortlich. Die Tatsache, dass die primäre Webpräsenz unter Rückgriff auf eigene Ressourcen vorgehalten wird, während die Fanpage unter Rückgriff auf die Dienste der Beigeladene praktisch ohne Aufwand unterhalten wird, ist unerheblich. In beiden Fällen ist die Klägerin für die Datenverarbeitung, die durch den Betrieb der Webseite ausgelöst wird, verantwortlich: Bezüglich der primären Webseite, weil sie die Datenverarbeitung selbst durchführt, und für die Fanpage, weil sie die Datenverarbeitung durch Dritte durchführen lässt. Die Verantwortlichkeit folgt in beiden Fällen aus § 3 Abs. 7 BDSG.

Ein abweichendes Ergebnis würde zu der Situation führen, dass die Klägerin sich dadurch ihrer Verantwortung für die auf einer von ihr betriebenen Webseite verarbeiteten Nutzungsdaten entziehen könnte, indem sie sich möglichst unzuverlässige und kooperationsunwillige Infrastrukturanbieter wählt bzw. keinerlei Interesse daran artikuliert, wie die ausgewählten Infrastrukturanbieter mit den dabei erlangten Nutzungsdaten ihrerseits umgehen. Datenschutzrechtlich soll diese Situation aber gerade durch die Regelungen der Auftragsdatenverarbeitung vermieden werden.

2.3.2 Rein vorsorglich: Störerhaftung

Eine Auffassung, die bei klar erkannter Rechtswidrigkeit der Datenverarbeitung des Infrastrukturdienstleisters sowohl zur Ablehnung einer Verantwortlichkeit als auch zur Ablehnung einer Störerhaftung gelangt, führte zu einer immensen Rechtslücke und wäre widersinnig. Selbst wenn man der Auffassung des Beklagten vom Vorliegen einer Auftragsdatenverarbeitung nicht folgen wollte, muss daher jedenfalls unter Herbeiziehung der Rechtsfigur der Störerhaftung eine effektive Inanspruchnahme der Klägerin nach § 38 Abs. 5 BDSG möglich sein. Selbst Petri (abermals „Datenschutzrechtliche Verantwortlichkeit im Internet“ ZD 2015, S.103, 105), der unter irrtümlicher Ablehnung der Auftragsdatenverarbeitung eine Verantwortlichkeit zunächst ablehnt, erkennt doch die daraus resultierende Schutzlücke als nicht hinnehmbar. Petri versucht die abgelehnte Verantwortlichkeit zwar zunächst noch über einen mit Prüfpflichten und subjektiven Elementen angereicherten Mittelweg zu begründen:

> „Andererseits wird man den Wertungen der §§ 8-10 TMG sowie der geschilderten Vorschriften im BDSG auch nicht gerecht, wenn der Fanpagebetreiber von seiner datenschutzrechtlichen Verantwortlichkeit völlig freigestellt wird.
> Im Ergebnis wird der Fanpagebetreiber aus § 9 BDSG heraus zu einer Prüfung der Zuverlässigkeit seiner Vertragspartner jedenfalls dann verpflichtet sein, wenn ein konkreter Anlass besteht, der die Zuverlässigkeit seines Vertragspartners infrage stellt. Das ist namentlich der Fall, wenn der Betreiber positiv um die datenschutzrechtliche Unzuverlässigkeit seines Vertragspartners weiß. Vergleichbares gilt, wenn er durch die betroffene Person oder durch seine zuständige Aufsichtsbehörde als unabhängiger Sachwalter von

> Betroffenenrechten (dort Fn 24 mit Hinweis auf BVerfGE 65,1, 46 zum vorgezogenen Rechtsschutz durch die Datenschutzaufsichtsbehörden, RA) auf die rechtswidrige Verletzung von Persönlichkeitsrechten hingewiesen wird."

und kommt dann in Zusammenfassung seiner Überlegungen zu einer abgestuften Verantwortlichkeit (S. 106):

> „Anders ist die Rechtslage, wenn Diensteanbieter bei der Verarbeitung personenbezogener Daten auf vertraglicher Basis bewusst arbeitsteilig vorgehen, z.B. indem ein Anbieter eine Kommunikationsplattform bereit stellt und ein anderer Anbieter diese Plattform nutzt, um Inhalte anzubieten. In einem solchen Fall führen notwendigerweise wechselbezügliche Datenverarbeitungen zu einer abgestuften datenschutzrechtlichen Verantwortlichkeit. Dabei ist jeder Anbieter für seine eigene Verarbeitung personenbezogener Daten selbst verantwortlich. Eine Verantwortlichkeit besteht jedoch auch insoweit, wenn der Anbieter nicht auf die positive Kenntnis von Tatsachen reagiert, die eine rechtswidrige Verarbeitung des jeweils anderen Anbieters begründen. In diesem Fall wird eine datenschutzrechtliche Verantwortlichkeit beider Anbieter begründet.
>
> Ein Spezialfall bildet eine bewusste arbeitsteilige Datenverarbeitung, welche die Voraussetzungen einer Auftragsdatenverarbeitung nach § 11 BDSG erfüllt. In diesem Fall weist § 11 Abs. 1 BDSG für das Außenverhältnis die datenschutzrechtliche Verantwortlichkeit weitgehend dem Auftraggeber zu."

Diese vermittelnde Ansicht ist aber abzulehnen, da sie keine Stütze im Gesetz findet. Das Vorhandensein eines Elements positiver Kenntnis von der Rechtswidrigkeit wird von Petri zu Unrecht zur Bedingung einer Anordnung nach § 38 Abs. 5 BDSG gemacht. Sie ist zudem unnötig, da entgegen Petris Auffassung im hiesigen Verfahren gerade ein Vertrag zwischen Klägerin und Beigeladener existiert, der eine Verantwortlichkeit bereits nach der üblichen Systematik des BDSG begründet. Petris Versuch, nach seiner Ablehnung der Auftragsdatenverarbeitung über Elemente der Kenntnis und Sorgfaltspflichten doch zu einer Verantwortlichkeit zu gelangen, zeigt aber, dass Petri erkennt, dass die bewusste Ausnutzung rechtswidriger Angebote nicht dazu führen kann, dass die so handelnde Stelle sich korrigierender Maßnahmen entzieht. Seine vermittelnde Auffassung ist damit für die Frage der Verantwortlichkeit zwar abzulehnen, für die Frage der Störerhaftung hingegen zu unterstützen. Die von

ihm postulierte Verantwortlichkeit (ZD 2015, S. 106) aufgrund positiver Kenntnis ist schließlich nichts anderes als eine Störerhaftung:

> „Eine Verantwortlichkeit besteht jedoch auch insoweit, wenn der Anbieter nicht auf die positive Kenntnis von Tatsachen reagiert, die eine rechtswidrige Verarbeitung des jeweils anderen Anbieters begründen. In diesem Fall wird eine datenschutzrechtliche Verantwortlichkeit beider Anbieter begründet."

Zu dieser Störerhaftung im Datenschutzrecht führt Petri deshalb im Falle jeder Ablehnung einer Verantwortlichkeit schließlich selbst aus (S. 105):

> „Sofern man entgegen der hier vertretenen Meinung eine datenschutzrechtliche Verantwortlichkeit des Anbieters einer Fanpage verneint, müsste zumindest nach den Maßstäben der Autocomplete-Entscheidung sowie der RSS-Feed Entscheidungen des Bundesgerichtshofs eine Störerhaftung geprüft werden. Setzt man voraus, dass der Anbieter der Infrastruktur Datenschutzrechte von Nutzern nachhaltig verletzt, kann der Fanpagebetreiber wohl schon als Störer herangezogen werden. Denn er fördert mit der Einrichtung und Nutzung der Fanseite adäquat kausal die mit Persönlichkeitsrechtsverletzungen einhergehende Infrastruktur. Es wäre dann widersinnig, ihn von einer Störerhaftung freizustellen, obwohl er einen erheblichen Nutzen aus der im Sinne des Persönlichkeitsrechts risikoträchtigen Infrastruktur ziehen kann. Hiervon zu unterscheiden ist die Frage, ob das im BGB verankerte allgemeine Persönlichkeitsrecht in derartigen Fällen auch als „sonstige Vorschrift über den Datenschutz" im Sinne des § 38 Abs. 1 Satz 1 BDSG anzusehen ist. Dafür mag immerhin sprechen, dass durch das zivilrechtliche Persönlichkeitsrecht auch die automatisierte Verarbeitung personenbezogener Daten (mit)geregelt wird."

Sollte also der Ansicht des Oberverwaltungsgerichts zu folgen sein, dass die Klägerin die für den Betrieb der eigenen Webseite notwendigen Daten weder durch eine eigene noch durch eine Verarbeitung im Auftrag durchgeführte Datenverarbeitung zu verantworten hat, muss die Inanspruchnahme jedenfalls nach den Grundsätzen der Störerhaftung rechtmäßig sein. Im Übrigen wird diesbezüglich erneut hilfsweise auf die Ausführungen in der Revisionsbegründung (S. 50ff) verwiesen.

2.4. Kein Ermessensfehlgebrauch durch den Beklagten

Der Beklagte hat schließlich auch sein Ermessen hinsichtlich der Inanspruchnahme der Klägerin fehlerfrei ausgeübt. Insbesondere war auch ein Vorgehen gegen die Beigeladene selbst nicht vorrangig geboten. Insoweit wird auf die Revisionsbegründung (S. 66 bis 70) verwiesen

Soweit das Oberverwaltungsgericht (US 20) ausführt,

> „die vom Beklagten behaupteten Verstöße könnten von Facebook ohne Weiteres beseitigt werden“,

ist zusätzlich darauf hinzuweisen, dass jedenfalls die auf die Safe-Harbor-Entscheidung gestützte Übermittlung der Nutzerdaten einen unheilbaren Datenschutzverstoß darstellt, der auch von der Beigeladenen rückwirkend nicht zu beseitigen ist, bzw. aktuell nur um den Preis der Einstellung ihres solchermaßen strukturierten Dienstes und damit auch Beendigung der Fanpage-Nutzung des Klägerin. Von einem Vorrang der Inanspruchnahme der Beigeladenen, wie offenbar die Beigeladene meint, kann schon deshalb nicht ausgegangen werden, weil für die Datenschutzverstöße durch die Beigeladene selbst der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit zuständig wäre, da die Facebook Deutschland GmbH in Hamburg ihren Sitz hat, und eine ermessensrechtliche Vorrangsprüfung immer nur die Verhältnisse im eigenen Zuständigkeitsbereich berücksichtigen kann und muss. Eine für das Ermessen zu berücksichtigende alternative Inanspruchnahme der Beigeladenen selbst scheidet somit aus.

Deshalb ist es für die Rechtmäßigkeit der streitigen Anordnung des Beklagten ohne Belang, dass neben der Fanpage der Klägerin noch weitere Webseiten auf Basis der Infrastruktur existieren. Die Argumentation der Beigeladenen im Schriftsatz vom 12.05.2015 (S. 97), dass die Deaktivierung der Fanpage keinen Einfluss auf die fortdauernde Nutzung des sozialen Netzwerks der Beigeladenen hätte, trägt nicht. Angesichts der weltweit großen Nutzerschaft wäre damit jedwedes Vorgehen gegen verantwortliche Stellen in Deutschland ausgeschlossen. Es ist widersprüchlich, wenn die Beigeladene einerseits vorträgt, dass nicht einmal die Deaktivierung aller Fanpages in Schleswig-Holstein eine wahrnehmbare Wirkung für die Rechte der Facebook-Nutzer hätte, während sie das entsprechende Ausbleiben von

Nutzerzugriffen als eine nicht hinnehmbare Wertminderung für ihr Netzwerk bezeichnet (S. 122).

Schließlich ist es auch irrelevant, dass die Beigeladene als unzuverlässige Auftragsdatenverarbeiterin gleichzeitig auch selbst verantwortliche Stelle sein kann. Verlässt ein Auftragsdatenverarbeiter den weisungsgebundenen Bereich und schwingt sich in Einzelbereichen gewissermaßen zum eigenen Herren über die Verarbeitungsvorgänge auf, wird er selbst verantwortlich für diese Verarbeitungsvorgänge (vgl. Petri, Simitis, Bundesdatenschutzgesetz, 8. Auflage, § 11, Rn. 89). Dies legt die Pflicht des Auftraggebers zur Einwirkung und – ultimativ – Beendigung der Zusammenarbeit aber nur umso mehr nahe. Die Tatsache, dass sich die Beigeladene mit einzelnen Bereichen ihres Geschäftsmodells außerhalb dessen befindet, was noch als weisungsabhängige Bereithaltung der Infrastruktur für die Klägerin angesehen werden muss, ändert an der Verantwortlichkeit der Klägerin für diejenigen Verarbeitungsprozesse nichts, die Gegenstand des Nutzungsvertrages mit der Beigeladenen sind.

Diese Situation führt sodann zu der – gemessen an dem gesamten Geschäftsmodell der Beigeladenen – Gesamtbewertung, dass Klägerin und Beigeladene gemeinsam für die jeweiligen Verarbeitungsprozesse der Fanpage verantwortlich sind, worauf bereits in der Revisionsbegründung (S. 44) hingewiesen worden war.

2.5. Vorabentscheidungsverfahren nach Art. 267 AEUV

Zusätzlich zu den bereits in der Revisionsbegründung (S. 70ff) dargestellten zwei entscheidenden Fragen, stellt sich mit Blick auf die Rechtsgrundlage des § 38 Abs. 5 BDSG eine dritte Rechtsfrage, deren Vorlage gemäß Art. 267 AEUV angeregt wird:

> Steht die Richtlinie 95/46/EG einer Regelung im nationalen Recht entgegen, durch die die Anordnung einer Maßnahme deswegen als Untersagung eines Verfahrens zu bewerten ist, weil sich der Inhalt der Anordnung in seinem Wortlaut auf eine Unterlassung anstatt einem positiven Tun bezieht, und die Anordnung einer solchen Unterlassung nur unter höheren Anforderungen als das positive Tun angeordnet werden kann?

3. Abschließend

Die Beigeladene hat in ihrer Stellungnahme erhebliche Kritik an manchen Ausführungen in der Revisionsbegründung geäußert. Soweit Ausführungen missverständlich waren, sollten diese durch vorstehenden Vortrag präzisiert worden sein.

An dieser Stelle wird ausdrücklich für den Hinweis der Beigeladenen auf die unrichtige Zitierung von Piltz (2014) in der Revisionsbegründung (S. 53) gedankt. Hier war es bei der Erstellung der Revisionsbegründung zu einem redaktionellen Fehler gekommen.

Dies ändert jedoch nichts an der datenschutzrechtlichen Kritik und den datenschutzrechtlichen Bedenken, die vom Bekl. an der Nutzung der Facebook-Infrastruktur durch die Klägerin dargelegt wurden.

Der guten Ordnung halber wird zu einigen Ausführungen der Beigeladenen in der gebotenen Kürze Stellung genommen. Dabei handelt es sich insbesondere um folgende Äußerungen:

- der Vorwurf, die Beigeladene informiere nicht zureichend über die Verwertungen der in der Kommunikation mit der Kl. von der Beigeladenen erlangten Daten (S. 26f Schriftsatz der Beigeladenen)

Dieser Vorwurf steht in Zusammenhang mit dem von der Kl. und der Beigeladenen durchgehend vorgebrachten Einwand, dass bereits bei Facebook registrierte Nutzer durch die einer Registrierung notwendigerweise vorangehenden Zustimmung zu den Datenverwendungsrichtlinien eine ausreichende Einwilligung für die hier in Rede stehenden Datenverarbeitungsvorgänge erteilt hätten.

Der Beigeladenen ist zuzugestehen, dass sie ihre Richtlinien immer wieder und den sich entwickelnden datenschutzrechtlichen Sensibilitäten entsprechend anzupassen sucht. Zur trotzdem unzureichenden Qualität dieser Einwilligungserklärung hat der Bekl. bereits ausführlich in der Revisionsbegründung vorgetragen (S. 25 ff). Auch sind in der von van Alsenoy u.a. vom Interdisciplinary Centre for Law and ICT (ICRI) der Katholischen Universität Leuven veröffentlichten Studie

Anlage B 10: From social media service to advertising network, A critical analysis of Facebook's Revised Policies and Terms, Draft 25.08.2015 "

massive Zweifel daran geäußert worden, ob sowohl die im Zeitpunkt des Erlasses des hier angegriffenen Bescheides geltenden Einwilligungsformeln als auch deren neueste Fassung 2015 dem Erfordernis einer informierten Einwilligung genügen (S. 12-17).

Dass die von der Beigeladenen verwandten Einwilligungsformeln nicht den Anforderungen genügen, die an eine „informierte Einwilligung" zu stellen sind, davon zeugt auch das gegen die Beigeladene am 26.10.2014 ergangene und rechtskräftige Urteil des Landgerichts Berlin (insbes. S. 9f), das vom Dachverband der 16 Verbraucherzentralen der Bundesländer und weiterer Verbraucherorganisationen erstritten worden ist.

Anlage B 11: Urteil LG Berlin vom 26.10.2014 – 16 0 60/13

Im Fall der Setzung von datr-Cookies bei nicht-Facebook-registrierten Besuchern der Fanpage der Klägerin fehlt es zudem - wie unter Bezugnahme auf das Urteil des Urteil des Dutch-Speaking Court of First Instance Brussels vom 09.11.2105 ausgeführt wurde - von vorneherein an einer ausreichenden Einwilligung.

- Vorwurf der Überinterpretation (S. 28 SS der Beigel.)

Die Beigeladene wirft dem Beklagten vor, das OVG-Urteil zu überinterpretieren. Das mag aus ihrer Sicht so sein. Tatsächlich hat sich das OVG nicht dem Sinne geäußert, wie es die Beigeladene sieht, sondern lässt das angegriffene Urteil die Auslegung des Beklagten zu.

- Vorwurf „bedenklichen Umgangs mit Recht und Gesetz" (S. 33)

Die Beigeladene vermischt mit ihrem Vorwurf die verschiedenen rechtlichen Ebenen zu durchsichtigem Zweck, wenn sie behauptet, der Bekl. würde „gegen seine eigene Rechtsüberzeugung" versuchen, „die streitige Anordnung mit dem Argument eines öffentlich-rechtlichen Kontextes zu retten". Unstreitig ist die Kl. eine Institution des privaten Rechts und unterliegt als solcher der Kontrollkompetenz des Bekl. über den privaten Bereich. Hiernach bemisst sich die Datenverarbeitung der Klägerin zweifellos nach den für den privaten Bereich geltenden Vorschriften des

Bundesdatenschutzgesetzes. Bereits nach diesen Vorschriften ist nach Beklagten-Auffassung der Betrieb der Fanpage der Kl. rechtswidrig und damit der vom Bekl. ausgesprochenen Sanktion gem. § 38 Abs. 5 BDSG verfallen. Hierzu bedarf es keines Rückgriffs auf eine öffentlich-rechtliche Pflichtenlage. Eine solche öffentlich-rechtliche Pflichtenlage führt aber bei der Wahrnehmung öffentlich-rechtlicher Aufgaben im Gewande des Privatrechts zu einer gesteigerten Pflicht der Beachtung der privatrechtlichen Normen, um Verletzungen von Grundrechten der Betroffenen möglichst zu vermeiden. Diese zusätzliche Pflichtenlage ist im Falle der Kl. gegeben und kann selbst bei im strikten Sinne privatrechtlich zulässigen Verhaltensweisen letztlich zu deren Unzulässigkeit führen.

Wo aber die Bewertung privatrechtlicher Verhaltensweisen in Streit steht und noch keine eindeutige und gefestigte Rechtsanschauung besteht, sondern erst im Werden ist, da führt die öffentlich-rechtliche Pflichtenlage dazu, Abstand von solchermaßen zweifelhaften Praktiken zu nehmen. Dieses Risiko darf nicht auf dem Rücken der Bürgerinnen und Bürger und deren Grundrechte ausgetragen werden.

Die Beigeladene möge dem Bekl. nicht vorwerfen, dass er sich in der Ausübung seiner Kontrollfunktionen genau an den gegebenen einerseits privat-rechtlichen und andererseits öffentlich-rechtlichen Rechtsrahmen hält und dort eine Zusammenschau vornimmt, wo diese beiden Bereiche bei Akteuren wie der Klägerin tatsächlich vermischt sind.

Dr. Kauß
Rechtsanwalt

Anlagen: wie im Text erwähnt