Simulation einer EuGH-Verhandlung

Stellungnahme der Beklagten

Im Verlauf des Vorlageverfahrens vor dem EuGH bezüglich des Rechtsstreits zwischen dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) und der Wirtschaftsakademie Schleswig-Holstein GmbH (WAR) wird in der folgenden Abhandlung die Rechtsauffassung der ULD dargestellt werden. Hierbei sollen systematisch die einzelnen Vorlagefragen nacheinander rechtlich analysiert werden.

Grundsätzlich kann bereits festgehalten werden, dass für eine möglichst weite Auslegung der Datenschutzrichtlinie in Fragen der materiellen Rechtslage und der räumlichen Anwendbarkeit zu plädieren ist, um einen möglichst umfassenden, harmonisierten und effektiven Datenschutz in Europa zu ermöglichen.

I. Vorlagefrage 1

Für die Frage der Rechtmäßigkeit der Deaktivierungsanordnung ist zunächst relevant, ob die Adressatin der Anordnung auch für die ihr zugrundeliegenden mutmaßlichen Verstöße gegen die Datenschutzvorschriften verantwortlich ist. Der Begriff des "für die Verarbeitung", und somit auch für die rechtswidrige Verarbeitung "Verantwortlichen" wird in Artikel 2 lit. d RL 46/95/EG bestimmt als die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Sollte die Klägerin nach den Bestimmungen dieser Datenschutzrichtlinie als verantwortlich gesehen werden können, wird auch bei der Anwendung der nationalen Datenschutznormen im Zuge einer europarechtskonformen Auslegung der gleiche Maßstab anzulegen sein.

Die Frage, ob die Klägerin unter oben genannte Definition eines für die Datenverarbeitung Verantwortlichen überhaupt fällt, kann jedoch dahinstehen, da Art. 2 lit. d keineswegs abschließend den Kreis Verantwortlicher Personen bestimmt, sondern lediglich beispielhaft seinen Regelfall nennt.

Dies folgt notwendigerweise aus dem Telos, der der Datenschutzrichtlinie zugrundeliegt. Dabei ist zunächst der Begriff der Verarbeitung näher zu untersuchen. Denn Art. 2 lit. d grenzt den Bereich der rechtlichen Verantwortlichkeit ab, indem er eine Qualitative Abstufung der Einwirkungsmöglichkeiten im Verarbeitungsprozess macht. Wer also eine hohe Einwirkungsmöglichkeit auf Mittel und Zweck der Verarbeitung hat, ist Verantwortlicher, wem diese fehlt, ist nicht verantwortlich. Keine Abgrenzung nimmt der Normentext jedoch vor was die Abgrenzung des Verarbeitungsprozesses nach vorne und hinten angeht, d.h., wo Verarbeitung anfängt und wo diese aufhört. Deshalb erscheint es als nicht vertretbar, die Verantwortlichkeit abzulehnen, weil Einwirkungsmöglichkeiten während eines Teilaktes der

Datenverarbeitung im engeren Sinne fehlt, wenn während eines für die Verarbeitung ebenso unentbehrlichen Teilakts volle Einwirkungsmöglichkeit bestand.

Einen solchen unentbehrlichen Teilakt der Datenverarbeitung stellt die Datenbeschaffung dar. Verarbeitung und Erhebung von Daten sind notwendigerweise miteinander gekoppelt, denn kann die Erhebung mitunter auch für sich alleine stehen, ist die Verarbeitung von Daten ohne ihre Vorherige Beschaffung nicht denkbar.

Im vorliegenden Fall hat die Klägerin durch anwerben von Nutzern ihrer Fanpage und bereitstellen von Inhalten, die konsumiert, kommentiert und geteilt werden konnten, einen erheblichen aktiven Part bei der Datenerhebung gespielt und hierbei auch im eigenen Interesse gehandelt. Die Behandlung von Art. 2 lit. d als abschließenden Katalog würde insofern zu dem Wertungswiderspruch führen, dass zwei rechtlich einander gleichwertige Sachverhalte unterschiedlich behandelt würden

Darüber hinaus ist die Unklarheit der auszulegenden Norm, die zu der hier diskutierten Streitfrage führt, mit ihrer Entstehungsgeschichte zu erklären, und gleichzeitig zu lösen.
Die Richtlinie 46/95/EG stammt aus dem Jahr 1995, einer Zeit, in der komplexe mehrstufige Informationsanbieterverhältnisse, in denen sämtliche Stufen miteinander interagieren, schlichtweg noch gar nicht vorstellbar waren. Dementsprechend kann der Gesetzgeber mit seiner Formulierung der Norm diese auch nicht auszuschließen gewollt haben. Vielmehr ist an dieser Stelle mehr denn je nach dem abstrakten Ziel des Gesetzgebers zu fragen, das ihn zur vorliegenden Norm bewegt hat. Mit seiner Formulierung hat er einen Adressatenkreis geschaffen, der im Jahre 1995 verhältnismäßig weitgefasst war. Insofern kann er nicht gleichzeitig bezweckt haben, dass sich dieser im Laufe der Zeit immer weiter verengt.

Vielmehr muss die Datenschutzrichtlinie evolutiv verstanden werden als eine Norm, die bewusst offen und eben nicht abschließend formuliert ist, um sich dem jeweiligen Zeitgeist anpassen und in einem Themenfeld, das sich erwartungsgemäß deutlich schneller entwickelt, als es jede Gesetzgebung leisten könnte, den notwendigen rechtlichen Rahmen bieten zu können. Diese Notwendigkeit ergibt sich vor allem aus der schieren Dominanz, die komplexe interaktive Informationssysteme, allen voran die sozialen Netzwerke, seit Jahren in nahezu allen gesellschaftlich erheblichen Sparten, von Unterhaltung über Kommunikation bis hin zu Vermarktung von Produkten, ausübt. Es kann nicht Ziel des Gesetzgebers gewesen sein, eine dermaßen große Gruppe von Akteuren in seiner Regelung außen vor zu lassen.

Selbst, wenn aber genau dies sein Ziel gewesen wäre, so wäre es heutzutage doch in einem gänzlich anderen Licht zu betrachten. Denn seit der Ratifizierung der europäischen Grundrechtecharta im Jahr 2009 ist Unionsrecht nicht nur historisch korrekt, sondern vor allem auch grundrechtskonform auszulegen. Die Datenschutzrichtlinie ist hierbei insbesondere im Lichte der Artikel 7 und 8 der europäischen Grundrechtecharta zu betrachten.

Art. 8 GrCH begründet ein europäisches Datenschutzgrundrecht, das jedenfalls bei Anwendung von Unionsrecht, wie hier der Datenschutzrichtlinie, auch von deutschen Gerichten beachtet werden muss. Die Konsequenzen der Einführung des Datenschutzgrundrechts für die Interpretation der Richtlinie hat der EuGH bereits in seinem Urteil zum Österreichischen Rundfunk deutlich gemacht.

Der Anwendungsbereich der Richtlinie ist, so der EuGH, sehr weit zu fassen, da Art. 8 GrCh einen vollumfänglichen Datenschutz gebietet. Bei konsequent enger und abschließender Anwendung bewirkt die Richtlinie allerdings alles andere als einen vollumfänglichen Datenschutz, sondern bestenfalls eine minimale Untergrenze, die die Mitgliedstaaten nicht unterschreiten sollen. Dies kann man exemplarisch sehr gut am vorliegenden Fall beobachten, der in seiner konkreten Ausgestaltung allein deshalb entstehen konnte, weil sich deutsches und irisches Datenschutzrecht trotz unionsrechtlicher Harmonisierung erheblich voneinander unterscheiden. Folglich ist die Datenschutzrichtlinie in der Weise zu interpretieren und nötigenfalls ergänzend auszulegen, dass ein Vollumfänglicher Schutz des Datenschutzgrundrechtes in sämtlichen Mitgliedstaaten gewährleistet ist.

Die Gewährleistung von Grundrechtsschutz kann sich jedoch nicht auf die bloß abstrakte Garantie von Rechten beschränken, sondern muss im Sinne einer Schutzpflicht des Staates auch die wirksame Durchsetzung dieser Rechte, nicht zuletzt vor dem Hintergrund des effet-utile-Grundsatzes, ermöglichen. Hierbei leuchtet ein, dass, je enger der Kreis derjenigen gezogen wird, die für einen Datenschutzrechtlichen Verstoß verantwortlich gemacht werden können, mit der Konsequenz, dass sie nicht zur Behebung des Verstoßes verpflichtet sind, desto mehr der Datenschutz zu einem Grundrecht verkümmert, das lediglich auf dem Papier besteht.

Aus diesem Grund ist Art. 2 lit. d der Datenschutzrichtlinie in grundrechtskonformer Auslegung so zu verstehen, dass der Definierte Personenkreis, der für die Verarbeitung von Daten verantwortlich ist, lediglich beispielhaft aufgezählt und gerade nicht abschließen geregelt ist.

Dass es sich bei dieser Auslegung nicht etwa um eine unzulässige richterliche Rechtsfortbildung handeln würde, unterstreicht schon die Tatsache, dass eine ähnliche Konzeption der Verantwortlichkeit für Datenschutzverstöße auf dem Gebiet des Zivilrechts bereits durch die Zivilgerichtsbarkeit in der Gestalt der mittelbaren Störereigenschaft eingeführt worden ist. Die Notwendigkeit einer weiter gefassten Zurechenbarkeit von Datenschutzverstößen steht demnach schon seit längerem auf der Tagesordnung.

Folglich wären grundsätzlich auch Maßnahmen gegen Personen rechtmäßig, die nicht unmittelbar über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheiden, soweit dies gesetzlich vorgesehen ist. Eine solche Ermächtigungsgrundlage kann

in Art. 28 III Spstr. 2 (in Form einer europarechtlichen Auslegungshilfe für die nationalen Ermächtigungsnormen) gesehen werden. Dieser garantiert den nationalen Datenschutzbehörden bestimmte Einwirkungsbefugnisse, darunter die Stellungnahme, die Aufforderung zur Stellungnahme, die Verwarnung datenschutzwidrig handelnder Stellen, sowie die die Sperrung, Löschung oder Vernichtung von Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung. Diese Befugnisse sind lediglich beispielhaft aufgezählt, was Formulierungen wie „oder“ und „beispielsweise“ nahelegen, und sehen explizit ein Ermessen der mitgliedstaatlichen Behörden vor. Es wird also ein sehr weitgefasstes Verständnis der Behördenbefugnisse gezeigt. Zu dieser Einschätzung passt, dass keinerlei Einschränkungen bezüglich des Adressaten der aufgelisteten Maßnahmen vorgenommen werden. Nachdem festgestellt wurden, dass die Wertung des Art. 2 lit. d die Befugnisse aus Art. 28 III Spstr. 2 nicht einzuschränken vermag, bereitet die weite Konzeption, die diese Norm von Behördenbefugnissen zeichnet, den Weg für die Haftung eines lediglich mittelbar Verantwortlichen für die rechtswidrige Verarbeitung personenbezogener Daten.

Sollte das Gericht entgegen unserer Auffassung entscheiden, dass Art. 2 lit. d als abschließende Norm zu verstehen ist, so muss nichtsdestotrotz festgehalten werden, dass diese Frage für die Beurteilung des Ausgangsverfahren nicht entscheidungserheblich und mithin obsolet ist. Denn unbeschadet einer engen Auslegung ist die Klägerin bereits als juristische Person i.S.d. Art 2 lit. d zu klassifizieren, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.

Mit Einrichten ihrer Fanpage setzt sie nämlich eine Bedingung, ohne die die Fraglichen Daten weder erhoben noch verarbeitet worden wären. Beim Setzen dieser Bedingung war sie sich in vollem Umfang über die Mittel im klaren, die Facebook bei der Datenverarbeitung und hat sie somit mittelbar gebilligt. Schließlich bezweckte sie mit Ihrem Handeln die Förderung der eigenen Interessen, nämlich die Auswertung der fraglichen Daten über Facebook Insights.

I. Vorlagefrage 2

Für den Fall, dass den Ausführungen in (I.) nicht gefolgt und eine Rechtmäßigkeit der behördlichen Anordnung aufgrund einer direkten Verantwortlichkeit der Klägerin für die angemahnten Datenrechtsverstöße abgelehnt wird, kommt immernoch eine Verantwortlichkeit wegen fahrlässig fehlerhafter Auswahl des Geschäftspartners innerhalb eines Auftragsverhältnisses zur Datenverarbeitung i.Sd. Art. 17 II der Datenschutzrichtlinie infrage.

Dieser sieht vor, dass eine Verantwortlichkeit auch für solche Handlungen besteht, die nicht selbst und unmittelbar vorgenommen werden, sondern vielmehr durch einen Dritten. Hierbei soll den Auftraggeber die Pflicht treffen, einen Auftragsverarbeiter auszuwählen, der

hinsichtlich der für die Verarbeitung zu treffenden technischen Sicherheitsmaßnahmen und organisatorischen Vorkehrungen ausreichende Gewähr bietet.

Die Vorlagefrage erwägt die Möglichkeit, dass die Tatsache, dass in dieser Norm von einem Auftragsverhältnis ausgegangen wird, im Umkehrschluss eine Sorgfaltspflicht bei der Auswahl (mit-)verarbeitender Dritter außerhalb eines expliziten vertraglichen Auftragsverhältnisses ausschließen könnte. Dieser Schluss erscheint allerdings als verfehlt, da er sich einzig und allein auf einen Wortlaut stützt, der zu wenig eindeutig ist, als dass man ihn als absolut betrachten könnte. Zwar bildet der Wortlaut die Grenze der Auslegung einer Norm, innerhalb dieser Auslegung ist allerdings in besonderem Maße auch der Telos zu berücksichtigen.

Sinn und Zweck des Artikel 17 II der Datenschutzrichtlinie ist es, zu verhindern, dass sich Rechtsakteure der Verantwortlichkeit für ihr Wirken zu entledigen, indem sie Dritte zwischenschalten, die „schmutzigen“ Aufgaben und damit die unmittelbare Datenverarbeitung für sie übernehmen. Für diese rechtsmissbräuchliche Flucht vor der Inanspruchnahme durch die Datenschutzbehörden ist kein klassisches vertragliches Auftragsverhältnis vonnöten. Ein synallagmatischer Austausch von Interessen kann auch dort entstehen, wo die Datenverarbeitung lediglich eine Nebenpflicht darstellt, oder in beiderseitigem Interesse geschieht. Das Entstehen eines solchen Profits, also einer Nährung der eigenen Interessen durch andere, ohne expliziten Auftrag, tritt typischerweise in Dreiecksverhältnissen auf, die wiederum mittlerweile den Regelfall komplexer Informationsanbieterverhältnisse darstellen, wie sie mit Entstehung der sozialen Netzwerke eingeführt wurden. Dass dabei die Datenverarbeitung nicht explizit vereinbart wird, sondern vielmehr Teil der allgemeinen Geschäftsbedingungen ist, ändert nichts daran, dass diese Dreieckskonstellation das gleiche Missbrauchspotential verbirgt, das Art. 17 II gerade verhindern soll. Denn einen Nutzen von den zur Verfügung gestellten „Facebook Insights“ etwa hat ein Fanpage-Betreiber allemal. Und diesen bezahlt er auch mit der Anwerbung von Nutzern, die durch ihre „Clicks“ die Werbeattraktivität von Facebook steigern.

Insofern läge statt eines Umkehrschlusses bei Art. 17 II eher der Erst-recht-Schluss nahe, dass, wenn jemand verantwortlich gemacht wird, wenn er sorgfaltswidrig eines eigens ausgewählte Auftragsperson für die Datenverarbeitung aussucht, er erst recht verantwortlich sein muss, wenn er fahrlässig fremde Personen (im eigenen Interesse) gewähren lässt.

Die schiere Tatsache, dass jemand Daten hauptsächlich im eigenen Interesse verarbeitet, schließt darüber hinaus nicht aus, dass er dadurch gleichzeitig auch fremde Interessen fördert, in der Erwartung einer wie auch immer geschaffenen Gegenleistung. Alles andere würde auch den Schutzzweck der Norm unterlaufen. Denn Zweck einer Datenschutzrichtlinie kann nur sein, systematisch betriebenen Missbrauch von Datenverarbeitung zu unterbinden. Wird jedoch die Zurechenbarkeit einer rechtswidrigen Handlung geringer, je mehr Akteure daran beteiligt sind, desto größer ist der Anreiz für den Rechtsverkehr, möglichst komplexe Verarbeitungsnetze zu konstruieren und mithin die Datenschutzverstöße zu systematisieren.

Ein Datenschutz ohne Verantwortlichkeit von Beteiligten, die von Verstößen anderer profitieren, ist nicht nur nicht dazu geeignet, diese Verstöße zu unterbinden, sondern lädt geradezu dazu ein. Ein Dreiecksverhältnis, in dem profitierende Parteien auch haften, wird hingegen effektiv Verstöße unterbinden, da sich die Beteiligung an fragwürdigen Interessenketten nicht mehr rentieren würde. Da es im Sinne des Telos des Art. 17 II ist, Anreize zum Verzicht auf Datenschutzverstöße zu bieten, sprechen die besseren Argumente somit für eine weite Auslegung seines Anwendungsbereiches auch auf Fälle des Austauschs verarbeiteter Daten, die nicht als direkte Aufträge zur Verarbeitung von Daten zu klassifizieren sind.

Auch im vorliegenden Fall trifft die Klägerin trotz fehlendem Auftragsverhältnis eine Auswahlverantwortlichkeit, da sie personenbezogene Daten durch einen Dritten hat verarbeiten lassen, ohne auf die Datenverarbeitung Einfluss zu haben. Jedenfalls trifft sie deshalb die Pflicht, den Informationsanbieter, dessen sie sich bedient, sorgfältig auszusuchen, oder zumindest offensichtlich rechtswidrig handelnde Anbieter außen vor zu lassen, zumal sie als mittelbare Störerin willentlich und adäquat-kausal zur Verletzung der Rechte von Fanpage-Besuchern beigetragen hat. Die Behauptung, dass die relativ geringen Einflussmöglichkeiten auf den Verarbeitungsprozess ihrerseits die Vorwerfbarkeit mindern würde, kann sie deshalb nicht exkulpieren, weil sich der Vorwurf des Datenschutzverstoßes hauptsächlich auf die Verletzung von Informationspflichten stützt, auf die die Klägerin ebensoviel Einfluss hatte, wie die Beigeladene Facebook selbst. Denn, dass Facebook sogenannte Cookies auf Nutzercomputern speichert, und dass sie selbst auch davon profitiert, das hätte sie zwar nicht verhindern, wohl aber auch trotz fehlendem Auftragsverhältnis den Nutzern kommunizieren können.

II. Vorlagefrage 3

In seiner dritten Vorlagefrage möchte das Bundesverwaltungsgericht vom EuGH geklärt wissen, ob eine deutsche Datenschutzbehörde auch dann zuständig für die Datenschutzaufsicht ist, wenn das zu prüfende Unternehmen zwar mit einer Niederlassung in Deutschland tätig ist, die Datenverarbeitung an sich jedoch ausschließlich in deiner Niederlassung außerhalb Deutschlands veranlasst und ausgeführt wird. Diese Frage knüpft an die Regelung des Art. 4 Abs. 1 lit. a i.V.m. Art. 28 Abs. 6 der Datenschutzrichtlinie an, wonach eine mitgliedstaatliche Datenschutzbehörde auch für die Überprüfung solcher Handlungen zuständig ist, die weder nach dem Recht dieses Mitgliedsstaats zu beurteilen ist, noch von einer Person aus diesem Mitgliedstaat durchgeführt wird, jedoch auf seinem Hoheitsgebiet geschieht. Gefragt wird mit anderen Worten, ob die für die in Art. 4 Abs. 1 lit. a i.V.m. Art. 28 Abs. 6 geforderte Handlung die schiere Marktpräsenz in Kombination mit einer Handlung in einem anderen Mitgliedsstaat ausreicht.

Zu dieser Frage hat sich der EuGH bereits in verschiedenen vorausgegangenen Urteilen geäußert. Allen voran ist hier die Rechtssache „Google Spain“ zu nennen. In diesem Urteil hat der Gerichtshof Art. 4 Abs.1 lit. a dergestalt ausgelegt, dass für die Begründung der Zuständigkeit einer Behörde die schiere Existenz einer Zweigniederlassung des in Anspruch zu nehmenden Unternehmens in ihrem Zuständigkeitsgebiet ausreicht. Dies unter der Maßgabe, dass das Unternehmen als Verantwortlicher in einem anderen Staat selbst die Verarbeitung personenbezogener Daten vornimmt, diese Verarbeitung durch oben erwähnte Zweigniederlassung etwa durch Verkauf von Werbeflächen standortspezifisch gefördert oder fruchtbar gemacht wird. Die Zweigniederlassung kann also als für die Verarbeitung personenbezogener Daten verantwortlich gesehen werden, soweit diese Förderung den wesentlichen Teil ihrer geschäftlichen Tätigkeit darstellt.

Gegen die Anwendbarkeit dieses Urteils bei der Lösung der vorliegenden Frage könnte angebracht werden, dass im Fall von Google die verantwortlich gemachte Zweigniederlassung in Spanien die einzige auf europäischem Boden war, wohingegen sich in diesem Fall die Frage auf eine parallele Zuständigkeit von zwei unterschiedlichen nationalen Datenschutzbehörden abzielt, die insofern auch beide für die Durchsetzung von Unionsrecht sorgen könnten. Allerdings besteht kein Anlass, die in „Google Spain“ ausdrücklich sehr weit gefassten räumlichen Anwendungsbereich von Art. 4 Abs.1 lit. a wieder einzuschränken, nur, weil etwaige Rechtspolitische Erwägungen, die dem Urteil zugrunde lagen, nicht in jedem Anwendungsfall Wirkung zeigen. Konkret verläuft zwischen Facebook Deutschland, Facebook Irland und Facebook US eine ebenso untrennbare Verbindung wie zwischen Google Spain und Google US.

Diese Auffassung wird auch vom EuGH gestützt in der Rechtssache Amazon. Diese ist in der Ausgangskonstellation der vorliegenden Fragestellung insofern noch näher, als hier über die Verantwortlichkeit zweier Zweigstellen innerhalb der Europäischen Union zu entscheiden war. Der Gerichtshof hat hier entschieden, dass die Verarbeitung personenbezogener Daten dem Recht jenes Mitgliedsstaates unterliegt, auf den das Unternehmen seine Geschäftstätigkeit ausrichtet, wenn sich zeigt, dass das Unternehmen die fragliche Datenverarbeitung im Rahmen der Tätigkeiten einer Niederlassung vornimmt, die sich in diesem Mitgliedsstaat befindet.

Demnach hat der EuGH hier nicht nur die Zuständigkeit der Datenschutzbehörde aus dem Mitgliedsstaat der Zweigniederlassung bestätigt, sondern auch dessen Recht für anwendbar erklärt und somit das Marktortprinzip eingeführt. Konsequenterweise muss dies folglich auch für den der vorliegenden Frage zugrundeliegenden Fall bedeuten, dass nicht nur die Zuständigkeit der in Deutschland zuständigen Datenschutzbehörde zu bestätigen, sondern auch das deutsche Datenschutzrecht als anwendbar zu erklären sind.

Bestätigt wird diese Rechtsauffassung auch durch den EuGH im seinem Urteil zu „Weltimmo“, in dem er nochmals unterstreicht, dass Art. 4 Abs. 1 lit. a der Datenschutzrichtlinie so zu lesen

ist, 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.
Auch hiernach ist Facebooks Handeln somit an deutschem Recht zu messen.

Betrachtet man die bisherige Rechtsprechung des EuGH zusammenfassend, ist festzuhalten, dass er den räumlichen Anwendungsbereich des aufgrund der Datenschutzrichtlinie erlassenen nationalen Rechts wiederholt sehr weit verstanden hat, was aufgrund der Parallelität der Wertung aus Art. 28 Abs. 6 i.V.m. Art 4 Abs. 1 lit. a auch für die Zuständigkeit der aufgrund dieses nationalen Rechts verfassten Datenschutzbehörden gelten muss.

Folglich muss eine Datenschutzbehörde auch für solche Datenverarbeitung zuständig sein, die zwar ausschließlich in deiner Niederlassung außerhalb ihres Hoheitsgebiets veranlasst und ausgeführt werden, bei denen das verantwortliche Unternehmen jedoch auch über eine Niederlassung in Deutschland verfügt, deren Tätigkeit sich in die Zwecke der Datenverarbeitung einfügt.

III. Vorlagefrage 4

Unmittelbar an die Argumentation aus (III.) knüpft auch die vierte Vorlagefrage des Bundesverwaltungsgerichts an, die danach fragt, ob, nach geklärter Zuständigkeit für Datenverarbeitungsprozesse, die in einem anderen Mitgliedstaat stattfinden, Maßnahmen innerhalb dieser Zuständigkeit auch gegen diejenige Zweigniederlassung im Inland, deren Existenz in (III.) als konstitutiv für die Zuständigkeit dargelegt wurde, gerichtet werden können.

Die Ermächtigung zu solchem Handeln ist in einem Erst-recht-Schluss aus Art. 28 Abs. 6 i.V.m. Art 4 Abs. 1 lit. a in seiner Lesart aus (III.) zu sehen. Wenn schon Maßnahmen gegen Akteure rechtmäßig sind, die gar nicht auf dem Hoheitsgebiet der Behörde in Erscheinung treten, weil ihnen aufgrund einer unzertrennlichen Verbundenheit bezüglich der Verarbeitungszwecke die Präsenz einer Zweigniederlassung zugerechnet wird, dann müssen erst recht solche Maßnahme rechtmäßig sein können, die sich innerhalb dieses Zurechnungsverhältnisses gegen denjenigen Teilakteur richten, der selbst tatsächlich innerhalb des im Normalfall den Zuständigkeitsbereich begrenzenden Hoheitsgebiets agiert.

Die genannten rechtsdogmatischen Erwägungen werden nicht zuletzt durch rechtspolitische Anliegen gestützt, die außer Acht zu lassen das Ergebnis nicht nur unbillig, sondern geradezu rechtswidersprüchlich erscheinen ließe. Die oben erwähnte schwer vorhersehbare Entwicklung hin zur Entstehung komplexer, mehrgliedriger Informationssysteme wirkt sich

nicht nur stark auf die Wandlung des (legalen) Wirtschaftsverkehrs aus, sondern nicht zuletzt auf die Ausprägungen neuer Formen von Kriminalität. Wo früher kriminelle Handlungen vornehmlich auf einen direkten Vermögenszugewinn abzielten, wird es zunehmend lukrativer, sich in einem ersten Schritt zunächst auf den illegalen Erwerb personenbezogener Daten zu konzentrieren. Bei solchen Konstellationen sind grenzüberschreitende Sachverhalte eher der Regelfall als die Ausnahme. Die Zuständigkeit der Datenschutzbehörden auf die Grenzen ihres Staates zu beschränken, oder ihr Zugriffsrecht sogar innerhalb dieser Grenzen zu beschneiden, würde sie gleichzeitig auf dem Gebiet der digitalen Gefahrenabwehr handlungsunfähig machen, was ebenfalls für ein weites Verständnis ihrer örtlichen Zuständigkeit spricht.

IV. **Vorlagefragen 5 und 6**

Die fünfte und sechste Vorlagefrage sind sich in ihrer Problemstruktur sehr ähnlich und sollen deshalb in dieser Stellungnahme gemeinsam behandelt werden.
Sie behandeln die Frage nach einer Bindung der deutschen Datenschutzbehörden an die rechtliche Beurteilung derjenigen (5. Vorlagefrage), bzw. nach der Notwendigkeit einer Handlungsermächtigung durch diejenige mitgliedstaatlichen Behörde (6. Vorlagefrage), die in Fällen von (III.) und (IV.) ebenfalls zuständig sind, da die Verarbeitung der personenbezogenen Daten in ihrem Hoheitsgebiet geschieht.

Hierbei soll zunächst ein Ausblick auf die künftige Rechtslage gewagt werden. Denn die geplante und größtenteils bereits ausgearbeitete Datenschutzgrundverordnung wird aller Voraussicht nach u.a. ebendiese geschilderten Fallkonstellationen regeln.
Die Tatsache, dass sie erst frühestens im Jahr 2018 inkrafttreten wird, verhindert zwar ihre direkte Anwendung, bedeutet jedoch nicht, dass sie in den anzustellenden Erwägungen völlig außer acht zu lassen ist. Denn sie ist ein starkes und das aktuellste Indiz für den Willen des Gesetzgebers, und kann mithin helfen, auch den Telos hinter der Datenschutzrichtlinie besser zu durchdringen.

Der Gesetzesentwurf sieht in Art. 56 grundsätzlich die Möglichkeit einer parallelen Zuständigkeit mehrerer Datenschutzbehörden vor, was gegen die Notwendigkeit einer Handlungsermächtigung der einen an die andere zuständige Behörde spricht. Zwar soll es eine federführende Stellung desjenigen Mitgliedstaats geben, in dessen Hoheitsgebiet sich der Hauptsitzt des Adressaten der Maßnahme befindet. Allerdings ist für den Fall des Dissenses nicht etwa die Vetomöglichkeit vorgesehen, sondern vielmehr ein Streitbeilegungsverfahren nach Art. 65 DS-GVO. Ein gewisser Interessenausgleich auf Augenhöhe wird also auch hier durchaus vorgesehen.

Diese gesetzliche Wertung findet bereits in der Datenschutzrichtlinie ihren Ausdruck, genauer in Artikel 29. Die Tatsache, dass für Fälle der Meinungsverschiedenheit auch in Zuständigkeitsfragen nicht etwa der Vorrang der einen oder der anderen Stelle, sondern durch

Art. 29 die Einrichtung einer Datenschutzgruppe vorgesehen wird, die Stellungnahmen über die Interpretation der Richtlinie abgibt, spricht gegen das Ermächtigungsmonopol einer einzelnen Behörde. Vielmehr steht hiernach der konsensuale Interessenausgleich im Mittelpunkt. Diese Wertung ist auch rechtspolitisch nachzuvollziehen. Es wäre gefährlich für die Umsetzung des Datenschutzes, und damit eines europäischen Grundrechtes, wenn der Kontrollbehörde eines einzelnen Mitgliedstaates die Kontrolle auch über Aktivitäten anderer Aufsichtsbehörde erhalten würde. Vielmehr entspräche es dem unionsrechtlichen Grundsatz des effet utile, möglichst effektiv die Umsetzung von Unionsrecht zu fördern, je mehr Aufsichtsbehörden zusätzlichen Schutz garantieren würden. Dies gilt sowohl für die Frage nach der Handlungsermächtigung, als auch für die nach der Bindung an die rechtliche Beurteilung anderer Behörden.

V. Fazit

In der Gesamtschau der Erwägungen zu den einzelnen Vorlagefragen ist festzuhalten, dass insbesondere grundrechtliche Erwägungen anhand von Art. 8 GrCH, aber auch die Linie der bisherigen Rechtsprechung des EuGH etwa in den Rechtssachen Google Spain und Amazon, sowie die Tatsache, dass sich die Sachlage seit Inkrafttreten der Datenschutzrichtlinie gerade im Bereich des Datenschutzes rasant verändert hat, stark dafür sprechen, für eine möglichst weite Auslegung der Datenschutzrichtlinie in Fragen der materiellen Rechtslage und der räumlichen Anwendbarkeit zu plädieren.

Aus diesem Grund ist auch die Maßnahme der ULD gegen WAR, die Deaktivierungsanordnung der Facebook-Fanpage, die den Streitgegenstand im Ausgangsverfahren ausmacht, als rechtmäßig anzusehen.