Silvia C. Bauer

Kata Viktoria Eles

Datenschutz

Social Media – Vernetzung überall

A Einleitung

In heutigen Zeiten ist fast jedes Unternehmen im Internet präsent: Aufgrund der enormen Reichweite des *world wide web* wird ein beträchtlicher Adressatenkreis erreicht, dem mit relativ wenig Aufwand das Unternehmen, seine Produkte und nicht zuletzt seine Philosophie näher gebracht werden können. Dabei findet die Präsentation von Unternehmen schon lange nicht mehr nur auf der hauseigenen Homepage statt: Viele Unternehmen nutzen soziale Netzwerke wie *Facebook*, *LinkedIn*, *Youtube* und Co. für ihre Marketing- und Vertriebsstrategien. Zudem bewegen sich ca. 90 Prozent der Internetnutzer auf Social Media.[1] In der heutigen Vernetzung bieten *Facebook* und Co. daher eine brillante Chance, das Unternehmen gezielt ins Blickfeld von potenziellen Mitarbeitern und Kunden zu rücken.

In der Praxis zeigt sich, dass Unternehmen, deren Mitarbeiter oder auch die von diesen eingesetzten Dienstleister, wie Marketingagenturen oder Webseitenersteller, auch im Zeitalter der Digitalisierung im Umgang mit sozialen Netzwerken häufig nicht geschult sind. Dabei liegen in deren Nutzung viele rechtliche Fallstricke – nicht zuletzt in datenschutzrechtlicher Hinsicht. So verlangt das Datenschutzrecht z. B. den Abschluss von speziellen Verträgen mit Anbietern wie *Facebook*, dass Besucher der Webseiten bei bestimmten Verarbeitungen Einwilligungen erteilen, und es müssen umfassen-

1 *Remmertz*, MMR 2018, 507.

de Belehrungen über den Umgang mit den Daten im Netz erfolgen. Es mehren sich Gerichtsentscheidungen – unter anderem des Europäischen Gerichtshofs – die Unternehmen dabei immer neue Vorgaben diktieren.

Seit Inkrafttreten der Datenschutzgrundverordnung (DSGVO) im Mai 2018 sind zudem die Risiken von Bußgeldern erheblich gestiegen: Verstöße können mit bis zu 20 Mio. Euro bzw. 4 Prozent des weltweit erzielten Jahresumsatzes einer Unternehmensgruppe geahndet werden, Art. 83 Abs. 5 DSGVO. Die französischen Datenschutzaufsichtsbehörden haben z. B. gegenüber Google aufgrund eines Verstoßes gegen die Transparenz im Umgang mit Daten 50 Mio. Euro Bußgeld verhängt.[2] Um dieses Risiko zu minimieren, müssen Unternehmen Maßnahmen ergreifen, um bei der Nutzung von Social Media in datenschutzrechtlicher Hinsicht „compliant" zu sein.

Das ist allerdings nicht ganz einfach – nachfolgend werden daher an aktuellen Beispielen einige der Hürden dargestellt, die es z. B. bei dem Einsatz von Fanpages bzw. Social Plugins oder im Zusammenhang mit den Posts der eigenen Mitarbeiter zu nehmen gilt.

B Risiken bei dem Betrieb einer Facebook Fanpage

Zahlreiche Unternehmen nutzen *Facebook* und Co.[3], um zusätzlich zu ihrer Unternehmenswebseite in den sozialen Medien präsent zu sein und dort z. B. eine *Facebook*-Unternehmensseite zu schaffen. Das Unternehmen kann sich hier selbst, seine Produkte und Angebote präsentieren bzw. posten, aber auch – und das ist wesentlich – aktiv mit den eigenen „Fans" kommunizieren. Diese haben die Möglichkeit, dort publizierte Inhalte zu liken, zu retweeten oder mit anderen zu teilen – die Streuwirkung ist damit immens und der Adressatenkreis der eigenen Informationen erweitert sich stetig.[4]

Datenschutzrechtlich wirft der Betrieb einer solchen Fanpage allerdings einige Fragen auf, die jüngst Gegenstand von gerichtlichen Entscheidungen waren. Besucht ein Fan eine solche Seite, werden von *Facebook* Cookies auf dem Endgerät des Fans platziert und sowohl *Facebook* als auch der Betreiber der Seite erhalten – wenn auch teilweise anonymisiert – Informationen über das Nutzerverhalten. Dies wurde allerdings in der Vergangenheit weder von *Facebook* noch von dem Betreiber der Fanpage dem Besucher gegenüber so kommuniziert. Das Unabhängige Landeszentrum für Datenschutz in Schleswig-Holstein („ULD") hatte daraufhin eine Untersagungsverfügung aufgrund von Intransparenz erlassen – der Rechtsstreit endete vor dem EuGH.[5]

I. Verantwortlichkeit bei dem Betrieb einer Facebook Fanpage

Eine der grundlegenden Fragen bei dem Betrieb einer *Facebook*-Unternehmensseite ist, wer de facto für deren Betrieb und die Umsetzung der datenschutzrechtlichen Pflichten, wie z. B. die nach Art. 13 DSGVO erforderliche Information der Betroffenen, verantwortlich ist.

1. Begriffsbestimmung: Verantwortlichkeit im Sinne der DSGVO

a) Wer ist Verantwortlicher?

Die DSGVO definiert in Art. 4 Nr. 7 DSGVO den „Verantwortlichen" als denjenigen, der allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Eine *separate Verantwortlichkeit* (Controller-Controller) liegt dann vor, wenn die Parteien jeweils für sich, also unabhängig voneinander eigenständig über Zwecke und Mittel der Datenverarbeitung entscheiden und damit jeweils eigene Zwecke verfolgen. Für die Rechtmäßigkeit der Vorgänge ist es erforderlich, dass die Datenverarbeitung jedes Verantwortlichen auf einer ausreichenden Rechtsgrundlage beruht.[6] Damit muss die Verarbeitung z. B. für die Erfüllung eines Vertrags erforderlich sein, es müssen überwiegende berechtigte Interessen des Unternehmens an der Übermittlung im Vergleich mit den schutzwürdigen Interessen der betroffenen Person vorliegen oder die betroffene Person muss in die jeweilige Verarbeitung eingewilligt haben (siehe zu den Rechtsgrundlagen Art. 6 Abs. 1 DSGVO).

b) Was ist ein Joint Controller?

Die DSGVO sieht – im Gegensatz zur früheren Rechtslage – zudem die Möglichkeit vor, dass zwei Verantwortliche die Entscheidungen hinsichtlich der Zwecke und Mittel der Datenverarbeitung nicht allein, sondern **gemeinsam** treffen. In diesem Fall liegt eine *gemeinsame Verantwortlichkeit* vor (so genanntes *„Joint Controllership"*), Art. 4 Nr. 7, 26 Abs. 1 S. 1 DSGVO. Folge der gemeinsamen Verantwortlichkeit ist, dass zwischen den *Joint Controllern* eine Vereinbarung im Sinne von Art. 26 DSGVO zu treffen ist, worin u.a. die Einzelheiten der Datenverarbeitungsvorgänge und die Wahrnehmung

2 https://www.heise.de/newsticker/meldung/DSGVO-Verstoesse-Frankreich-verhaengt-Millionen-Strafe-gegen-Google-4283765.html.

3 Ebenso auch andere soziale Netzwerke, wie etwa LinkedIn, Xing, etc.

4 *Fuhlrott/Oltsmanns*, NZA 2016, 785 (786).

5 Vgl. zu den Vorinstanzen: VG Schleswig-Holstein, 9.10.2013 – 8 A 14/12 m. Anm. *Härting*, K&R 2013, 824 ff.; OVG Schleswig, 4.9.2014 – 4/LB 20/13; K&R2014, 831 ff.; BVerwG, 25.2.2016 – 1 C 28/14, K&R 2016, 437 ff..

6 *Thomas/Petri* in: Simitis/Hornung/Spiecker gen. Döhmann, 1. Auflage 2019, DSGVO Art. 4 Nr. 7 Rn. 4.

der Betroffenenrechte in transparenter Weise bestimmt werden müssen.[7] Jede Partei bleibt dabei weiterhin dafür verantwortlich, den durch die DSGVO normierten Pflichten nachzukommen. Wer welche Pflicht erfüllt und in welcher Höhe für was im Innenverhältnis gegenüber der jeweils anderen Partei haftet, wird in der Vereinbarung festgelegt. Bei einer Verletzung der Pflichten haften die Joint Controller gegenüber Betroffenen, die Schadersatz geltend machen, allerdings gesamtschuldnerisch, Art. 82 Abs. 2 S. 1, Abs. 4 DSGVO.[8]

Die Vereinbarung nach Art. 26 DSGVO stellt im Übrigen keine Rechtsgrundlage für den Austausch der Daten zwischen den beiden Parteien dar, die in der Regel bei einer gemeinsamen Verarbeitung von Daten erfolgt. Vielmehr muss auch die Übermittlung von einem Joint Controller an den anderen z. B. auf Basis einer der in Art. 6 Abs. 1 DSGVO aufgezählten Rechtsgrundlagen zulässig sein.[9]

c) Auftragsverarbeiter

Als dritte Alternative kennt die DSGVO die so genannte „Auftragsverarbeitung": Eine Auftragsverarbeitung nach Art. 4 Nr. 8 liegt vor, wenn personenbezogene Daten im Auftrag des Verantwortlichen durch ein anderes Unternehmen verarbeitet werden. Der Auftragsverarbeiter (Processor) ist nicht Verantwortlicher im Sinne der DSGVO, er fungiert lediglich als „verlängerter Arm" des jeweils Verantwortlichen. Aus faktischer Sicht hat der Auftragsverarbeiter zwar die Gewalt über den Verarbeitungsprozess, er bestimmt jedoch nicht final über die Zwecke und Mittel der Verarbeitung, sondern unterliegt letztendlich den Weisungen des Verantwortlichen.[10]

Der EuGH hat mit seiner aktuellen Rechtsprechung im Bereich des Social Media Rechts dieser Alternative eine Absage erteilt (→ unter B.I.2.) und erklärt im Umgang mit personenbezogenen Daten die verschiedenen Beteiligten jeweils zu Verantwortlichen bzw. Joint Controllern.

2. Rechtsprechung: *Facebook*-Fanpage Entscheidung

In der *Facebook*-Fanpage Entscheidung beschäftigte sich der EuGH erstmals seit Inkrafttreten der DSGVO mit den Voraussetzungen, unter denen eine gemeinsame Verantwortlichkeit (Joint Controller Relationship) im Rahmen von Social Media vorliegen kann.[11] Das Gericht stellte in seiner Entscheidung fest, dass der Betreiber einer *Facebook*-Fanpage und *Facebook* selbst gemeinsame Verantwortliche (Joint Controller) seien.[12]

Grund dafür sei, dass bei dem Aufruf einer Fanpage personenbezogene Daten der Besucher erhoben würden, die letztlich in einer Statistik erfasst würden, auf die auch der Betreiber zugreifen könne. Zwar seien die Daten in der Statistik anonymisiert, dennoch sei der Betreiber gemeinsam mit *Facebook* für diese Verarbeitung verantwortlich. Erst die Einrichtung der Fanpage ermögliche es *Facebook*, Cookies auf den Computern der Nutzer zu platzieren, durch die die Daten erhoben werden könnten. Zudem könne der Betreiber der Fanpage mittels Parametrierung mitentscheiden, welche Daten welcher Personen analysiert werden sollen.[13]

Dass der Betreiber der Fanpage nicht in allen Phasen des Datenverarbeitungsvorgangs Zugang zu den Daten habe, sei ebenfalls unschädlich, denn einer gemeinsamen Verantwortlichkeit stehe nicht entgegen, dass die Beteiligten nicht in gleichwertiger Art und Weise Zugang zu den personenbezogenen Daten hätten.[14] Außerdem profitiere der Betreiber der Fanpage durch die Nutzung der Daten, da er die Fanpage aufgrund der Ergebnisse optimieren könne.[15] Er nutze das soziale Netzwerk zu seinen Zwecken, unter Kenntnis der Nutzungsbedingungen und solle durch die Nutzung der Plattform (im Gegensatz zu seiner eigenen Homepage) nicht privilegiert werden.[16] Der Betreiber ermögliche auch die Verarbeitung der Daten von Nutzern, die keinen *Facebook*-Account hätten.[17] Somit sei der Betreiber maßgeblich an der Entscheidung der Mittel und Zwecke der Datenverarbeitung beteiligt. Im Ergebnis seien die Voraussetzungen des Art. 4 Nr. 7 Alt. 2 DSGVO erfüllt und es liege daher zwischen dem Betreiber der *Facebook*-Fanpage und *Facebook* eine gemeinsame Verantwortlichkeit vor.[18]

II. Folge für Unternehmen: Abschluss eines Vertrags, Belehrung, Prüfung der Rechtsgrundlagen, etc.

Unternehmen, die eine *Facebook*-Fanpage erstellen und betreiben, gelten gemeinsam mit *Facebook* als (Mit-) Verantwortliche im Sinne der DSGVO. Sie müssen

7 *Kartheuser/Nabulsi*, MMR 2018, 717.

8 *Kremer*, CR 225 (232).

9 *Lachenmann* in Koreng/Lachenmann, Formularhandbuch Datenschutzrecht 2. Auflage 2018, Art. 26 DSGVO, Rn. 1.

10 *Martini* in Paal/Pauly, DSGVO BDSG, 2. Auflage 2018, DSGVO Art. 28 Rn. 1 f.

11 Weitere Ausführungen zur gemeinsamen Verantwortlichkeit auch in der „Zeugen Jehovas"-Entscheidung: EuGH, Urteil vom 10.07.2018 – C-25/17, ZD 2018, 469.

12 EuGH, Urteil vom 05.06.2018 – C-210/16, MMR 2018, 591 Rn. 39.

13 EuGH, Urteil vom 05.06.2018 – C-210/16, MMR 2018, 591 Rn. 35 ff.

14 EuGH, Urteil vom 05.06.2018 – C-210/16, MMR 2018, 591 Rn. 43.

15 EuGH, Urteil vom 05.06.2018 – C-210/16, MMR 2018, 591 Rn. 34, 37.

16 EuGH, Urteil vom 05.06.2018 – C-210/16, MMR 2018, 591 Rn. 32, 40.

17 EuGH, Urteil vom 05.06.2018 – C-210/16, MMR 2018, 591 Rn. 35, 41.

18 EuGH, Urteil vom 05.06.2018 – C-210/16, MMR 2018, 591 Rn. 39, 44.

daher gemeinsam mit *Facebook* die Pflichten der DSGVO erfüllen und dazu ein Joint-Controller-Arrangement abschließen. *Facebook* hat inzwischen eine entsprechende Vereinbarung zur Verfügung gestellt; allerdings sehen die deutschen Datenschutzaufsichtsbehörden diese als nicht ausreichend an. Solange *Facebook* nicht nachbessere, sei ein datenschutzkonformer Betrieb der Fanpage nicht möglich. Zudem sei die erforderliche Transparenz im Umgang mit den Daten weiterhin nicht gegeben: *Facebook* stelle nicht klar dar, welche Verarbeitungen vorgenommen würden, so dass letztlich auch der Betreiber der Fanpage nicht ausreichend über die Verarbeitungen informieren und deren Zulässigkeit sicherstellen könne.[19]

Selbst wenn Unternehmen – soweit es ihnen eigenständig möglich ist – ihre Pflichten nach DSGVO erfüllen und z. B. eine Datenschutzerklärung entsprechend Art. 13 ff. DSGVO auf der Fanpage platzieren bzw. durch Setzen eines Links dort einfügen, ein Impressum vorhalten und über die einschlägigen Rechtsgrundlagen für die Verarbeitung bzw. den Austausch der Daten für u.a. werbliche Zwecke informieren, verbleiben bis zu einer Einigung zwischen *Facebook* und den Datenschutzaufsichtsbehörden Restrisiken.[20]

In diesem Zusammenhang stellt sich auch die Frage, ob sich diese Konsequenzen auch bei dem Betrieb von Unternehmensseiten auf anderen sozialen Netzwerken, wie z. B. *LinkedIn*,[21] ergeben. Abschließend geklärt ist dies nicht – allerdings weisen die Methoden von *LinkedIn* viele Parallelen zu *Facebook* auf: So ist auch bei *LinkedIn* die Erstellung einer Unternehmensseite möglich und aus der Datenschutzerklärung ergibt sich, dass dort ebenfalls Cookies eingesetzt werden – auch bei Nicht-Mitgliedern.[22] Aus diesen Daten werden wiederum Statistiken erstellt,[23] die für den Betreiber der Seite zugänglich sind. Zwar ist hier nicht ganz klar, ob der Seitenbetreiber durch das Setzen von Filtern mitentscheiden kann, welche Daten erhoben werden; er schafft gleichwohl die Möglichkeit, dass es überhaupt zu einer Datenerhebung kommt.

Die aktuelle Rechtsprechung zeigt, dass die Gewährleistung eines wirksameren und umfassenden Schutzes der personenbezogenen Daten der natürlichen Personen von höchster Priorität ist,[24] sodass der EuGH insgesamt zu einer sehr weiten Auslegung des Verantwortlichkeitsbegriffs tendiert[25] und auch zügig von einer gemeinsamen Verantwortlichkeit ausgeht. Daher ist es wahrscheinlich, dass auch bei Plattformen wie *LinkedIn* eine gemeinsame Verantwortlichkeit zwischen Seitenbetreiber und *LinkedIn* angenommen wird, sodass auch hier die Pflichten der DSGVO entsprechend berücksichtigt werden müssen. Soweit bekannt, zeigen diese Plattformen bislang allerdings wenig Neigung, mit den Betreibern die erforderlichen Joint-Controller-Arrangements abzuschließen. Insofern empfiehlt es sich abzuwarten, wie sich die Datenschutzaufsichtsbehörden diesbezüglich positionieren.

C Verknüpfung der eigenen Internetseite mit Social Media

Eine weitere Nutzungsmöglichkeit von Social Media im Unternehmen ist die Integration von so genannten „Social Plugins" auf der eigenen Webseite, wie z. B. des „Gefällt mir-Buttons" von *Facebook*. Wird dieser auf der Webseite z. B. unter ein Produkt platziert, können Besucher der Webseite durch Drücken des Buttons direkt auf *Facebook* bekunden, dass sie ein Produkt gut finden und diese Einschätzung mit anderen teilen. Dazu bauen Webseitenbetreiber den Programmcode für den Button in ihre Webseiten ein. Durch diesen Einbau werden allerdings auch Daten des Besuchers der Webseite, wie seine IP-Adresse oder Browserdaten, automatisch – also ohne Drücken des Buttons – an *Facebook* versandt. So kann z. B. deren Surfverhalten nachvollzogen werden. Dies gilt auch für Besucher, die keinen *Facebook*-Account haben.

Da diese Verarbeitung der Daten dem Besucher nicht transparent dargestellt wurde und erneut die Verantwortlichkeit für die Verarbeitung – *Facebook* oder Betreiber der Webseite bzw. beide gemeinsam – strittig war, kam es auch in diesem Zusammenhang zu einem Rechtsstreit, der durch den EuGH entschieden wurde.

I. Rechtsprechung: Fashion ID-Entscheidung

Die *Fashion ID GmbH & Co. KG*[26] hatte auf ihrer Webseite u.a. den „Gefällt mir"-Button von *Facebook* einge-

19 Siehe dazu den Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vom 1. April 2019; abrufbar unter: https://www.datenschutzkonferenz-online.de/media/dskb/20190405_positionierung_facebook_fanpages.pdf.

20 Impressumspflicht bei sozialen Netzwerken bejahend: OLG Düsseldorf, MMR 2014, 393; LG Regensburg MMR 2013, 246 m. Anm. Bienert; LG Trier MMR 2018, 112; vgl. auch *Härting/Gössling*, NJW 2018, 2523 (2526).

21 Ebenso auch Xing und Twitter.

22 Abrufbar unter: https://www.linkedin.com/legal/cookie-policy, zuletzt abgerufen am 06.08.2019.

23 Abrufbar unter: https://business.linkedin.com/de-de/marketing-solutions/linkedin-pages/best-practices?#, zuletzt abgerufen am 06.08.2019.

24 EuGH, Urteil vom 29.07.2019, – C-40/17; sowie EuGH, Urteil vom 10.07.2018 – C-25/17, ZD 2018, 469.

25 *Jung/Hansch*, ZD 2019, 143 (144).

26 Im Folgenden: Fashion ID.

bunden. Wie oben ausgeführt übermittelte der Browser des Besuchers bei Aufruf der Webseite dessen personenbezogene Daten automatisch an *Facebook* – ohne, dass es dem Besucher der Webseite bewusst war und auch unabhängig davon, ob der Besucher den „Gefällt mir"-Button drückte oder eine Mitgliedschaft bei *Facebook* hatte.[27]

1. Auch hier: Joint Controller Verhältnis

Wie bereits im Fall „Fanpage" erklärte der EuGH, dass der Drittanbieter (*Facebook*) und der Webseitenbetreiber (*Fashion ID*) gemeinsam für die Verarbeitung Verantwortliche, also Joint Controller, seien. In der Begründung bezog sich das Gericht mehrfach auf die bereits ergangenen Entscheidungen,[28] stellte jedoch noch einmal ausdrücklich klar, dass eine gemeinsame Verantwortlichkeit nicht zwingend zu einer gleichwertigen Verantwortlichkeit führe; der Grad der Verantwortlichkeit müsse für jeden Einzelfall unter Berücksichtigung aller maßgeblichen Umstände beurteilt werden.[29]

Im vorliegenden Fall entscheide *Fashion ID* mit über die Mittel, da erst durch die Einbindung der Social Plugins die Erhebung der Daten über ihre Webseite ermöglicht werde. Der gemeinsame Zweck folge daraus, dass es einerseits *Fashion ID* durch die Social Plugins ermöglicht werde, die Werbung für ihre Produkte zu optimieren und *Fashion ID* – um in diesen „wirtschaftlichen Genuss" zu kommen – jedenfalls stillschweigend in die Erhebung der personenbezogenen Daten ihrer Besucher durch *Facebook* eingewilligt habe. Dieser Verarbeitungsvorgang werde im wirtschaftlichen Interesse von beiden Parteien durchgeführt, sodass hierin der gemeinsame Zweck liege.[30]

Ein wichtiger Aspekt für eine Verantwortlichkeit von *Fashion ID* sei, dass die personenbezogenen Daten jedes Webseitenbesuchers übermittelt werden, also auch desjenigen, der keine *Facebook*-Mitglied sei. Daher würden Daten von Betroffenen durch *Facebook* erhoben, die selbst überhaupt keine Verbindung zu *Facebook* hätten. Daher sei es naheliegend, *Fashion ID* ebenfalls als Verantwortlichen einzuordnen.[31]

Allerdings grenzte das Gericht die gemeinsame Verantwortlichkeit auf diejenigen Vorgänge ein, an denen *Fashion ID* tatsächlich beteiligt war. Daher nahm das Gericht für den Vorgang der Datenerhebung eine gemeinsame Verantwortlichkeit an; für die nachfolgende Speicherung durch *Facebook* auf ihren Servern liege hingegen keine gemeinsame Verantwortlichkeit vor, für diese Verarbeitung sei *Facebook* allein verantwortlich.[32]

2. Erfüllung weiterer Pflichten durch den Betreiber der Webseite

Der EuGH ging daneben davon aus, dass in einer Joint-Controller-Beziehung derjenige, der in einer direkten Beziehung zum Betroffenen stehe – hier der Betreiber der Webseite – dafür Sorge tragen müsse, dass die Übermittlung der Daten an *Facebook* auf einer wirksamen Rechtsgrundlage erfolgt und dass er im Einklang mit Art. 13, 14 DSGVO den Besucher der Webseite umfassend über den Umgang mit den Daten informiert.[33] Ist daher eine Einwilligung für die Weitergabe der Daten erforderlich, muss der Betreiber der Webseite diese auch im Einklang mit den rechtlichen Voraussetzungen und nachweislich einholen.[34]

II. Folge für Unternehmen: Abschluss eines Vertrags, Belehrung, Prüfung der Rechtsgrundlagen, etc.

Im Ergebnis bleibt sich der EuGH seiner Rechtsprechung treu und verlangt von dem Betreiber der Webseite mit *Facebook* eine Joint-Controller-Vereinbarung abzuschließen, Besucher umfassend zu belehren und die erforderlichen Rechtsgrundlagen für den Umgang mit den Daten zu schaffen. Entsprechendes gilt auch für die Social Plugins anderer Anbieter.

Wer also Social Plugins auf seiner Webseite verwendet, sollte unbedingt darauf achten, die Datenschutzhinweise anzupassen und eine Vereinbarung im Sinne von Art. 26 DSGVO mit dem Anbieter des Social Plugins zu schließen.[35] Letzteres lässt sich in der Praxis – wie bereits oben ausgeführt – zurzeit eher schwierig bis gar nicht umsetzen.

Fällt gleichwohl die Entscheidung für deren Einsatz, und der Betreiber der Webseite holt zur Minimierung von Risiken eine Einwilligung in die Übermittlung der Daten ein, muss er darauf achten, dass der Besucher der Webseite diese vor einer Übermittlung der Daten an

27 EuGH, Urteil vom 29.07.2019 – C-40/17, Rn. 26 f.

28 *Facebook Fanpage*: EuGH, Urteil vom 05.06.2018 – C-210/16, MMR 2018, 591; *Zeugen Jehovas*: EuGH, Urteil vom 10.07.2018 – C-25/17, ZD 2018, 469.

29 EuGH, Urteil vom 29.07.2019 – C-40/17, Rn. 65 ff.

30 EuGH, Urteil vom 29.07.2019 – C-40/17, Rn. 75 ff.

31 EuGH, Urteil vom 29.07.2019 – C-40/17, Rn. 83; ähnlich schon in *Facebook Fanpage*: EuGH, Urteil vom 05.06.2018 – C-210/16, MMR 2018, 591.

32 EuGH, Urteil vom 29.07.2019 – C-40/17, Rn. 74.

33 EuGH, Urteil vom 29.07.2019 – C-40/17, Rn. 102, 103.

34 Teilweise wird hier auch argumentiert, dass ggf. aufgrund überwiegender berechtigter (=kommerzieller) Interessen des Betreibers der Webseite im Vergleich mit den schutzwürdigen Interessen des Betroffenen am Unterlassen der werblichen Ansprache die Daten an Facebook weitergegeben werden dürften, Art. 6 Abs. 1 lit. f DSGVO. Dann wäre eine Information des Betroffenen über diese Verarbeitung und sein Widerspruchsrecht (siehe Art. 13, 21 DSGVO) ausreichend. Der EuGH hat in seiner Entscheidung diese Rechtsgrundlage als Alternative jedenfalls nicht ausgeschlossen. Da die Datenschutzaufsichtsbehörden allerdings in diesem Zusammenhang eher zu Einwilligungslösungen tendieren, ergeben sich bei dieser Alternative gewisse Restrisiken.

35 *Hansen/Johnson*, GRUR.Prax 2019, 47.

Facebook erteilt. Damit dürfen die Social Plugins vor Erteilung der Einwilligung auf keinen Fall aktiviert sein. In der Praxis haben sich hier die sogenannte Zwei-Klick-Lösung bzw. die Shariff-Lösung durchgesetzt, die letztlich auch von den Datenschutzaufsichtsbehörden empfohlen werden.[36]

1. Zwei-Klick-Lösung

Bei der Zwei-Klick-Lösung wird der in Rede stehende „Like-Button" nicht jedem Besucher der Webseite angezeigt, sondern letztlich nur demjenigen, der sie aktiv nutzen möchte. Daher wird dem eigentlichen Plugin-Button ein anderer Button vorangestellt, der anzeigt, zu welchen Social Media Anbietern verlinkt werden kann. Der Besucher muss also zunächst die Social Plugins selbst aktivieren, um dann im zweiten Schritt die Inhalte auf den sozialen Netzwerken teilen zu können. In dem Moment, in dem der Besucher die Social Plugins aktiviert, werden die Daten an den Anbieter der Social Plugins übermittelt.[37] Die bewusste und eindeutige Aktivierung wird als Einwilligung interpretiert.

2. Shariff-Lösung

Bei der Shariff-Lösung werden die Social Plugins bereits bei dem Aufruf der Webseite angezeigt. Es handelt sich allerdings nicht um die eigentlichen Plugins, sondern nur eine funktionelle Nachbildung. Der Server der besuchten Webseite baut eine Verbindung zum sozialen Netzwerk auf – ohne die IP-Adresse des Besuchers zu übermitteln – und ruft die relevanten Informationen (zum Beispiel Anzahl der Likes) selbst ab, um diese dem Besucher anzeigen zu können. Erst, wenn der Besucher dann das Social Plugin nutzt, also beispielsweise ein Produkt selbst teilt, wird die IP-Adresse an das soziale Netzwerk übermittelt.[38]

D Social Media im Arbeitsverhältnis

Mitarbeiter des Unternehmens nehmen an dessen aktueller Entwicklung gerne teil und vernetzen sich daher häufig mit „ihrer" Unternehmensseite auf Social Media, liken über Social Plugins Inhalte oder teilen Fotos und Videos über ihre Netzwerke, die letztlich einen Bezug zum Unternehmen haben können.

Posten sie dabei z. B. Beiträge auf berufsbezogenen Netzwerken wie *LinkedIn* und Xing, ist es denkbar, dass die Unternehmensseite diese Beiträge teilt, um so die Aufmerksamkeit darauf zu lenken. Dieses Teilen ist ein „Re-Posten", also ein erneutes Hochladen – damit wird der Post einem größeren Empfängerkreis angezeigt. Teilt der Mitarbeiter dabei eher ungewünschte oder urheberrechtlich kritische Inhalte, kann dies zu einem bösen Erwachen bzw. ggf. zu einer eigenen Haftung des Unternehmens führen.

I. Meinungsfreiheit und ihre Grenzen

Auch wenn ein Großteil der Äußerungen des Mitarbeiters in Social Media – insbesondere in privaten Netzwerken – als Meinungsäußerungen, die von der Meinungsfreiheit nach Art. 5 Abs. 1 Grundgesetz gedeckt sind, interpretiert werden kann, steht dem die wirtschaftliche Betätigungsfreiheit des Arbeitgebers nach Art. 12 Abs. 1 Grundgesetz als ebenfalls schützenswertes Gut entgegen. Mitarbeiter können daher nicht bedenkenlos Aussagen über ihren Arbeitgeber in Social Media verbreiten; sofern sie gewisse Grenzen überschreiten, kann schon das Liken zu einer Haftung bzw. zu arbeitsrechtlichen Konsequenzen führen. Insbesondere in beruflichen Netzwerken kann der Arbeitgeber bei inhaltlichen Entgleisungen, falschen Äußerungen, etc. z. B. Unterlassung einfordern oder sogar das Arbeitsverhältnis kündigen.[39]

II. Gemeinsame Verantwortlichkeit durch Posten?

Fraglich ist allerdings, inwieweit er ggf. selbst haftet, wenn er es zulässt, dass seine Mitarbeiter beispielsweise Informationen posten, die er auf seinen Seiten teilt: Das Teilen von Inhalten ist nämlich als datenschutzrechtlich relevante Handlung einzuordnen, wenn personenbezogene Daten[40] geteilt werden. Ob aus datenschutzrechtlicher Sicht das Teilen eines Beitrages bereits zu einer (gemeinsamen) Verantwortlichkeit zwischen demjenigen, der die Plattform betreibt (d. h. dem Arbeitgeber) und demjenigen, der den ursprünglichen Post hochgeladen hat (d. h. dem Mitarbeiter), führt, ist noch wenig diskutiert. Vor dem Hintergrund der Entscheidungen des EuGH scheint die Tendenz eher in Richtung großzügige Auslegung der gemeinsamen Verantwortlichkeit zu gehen; davon ausgehend würde ggf. bereits ein gemeinsam verfolgtes Ziel für eine entspre-

36 *Lachenmann* in Koreng/Lachenmann, Formularhandbuch Datenschutzrecht, F.I.6. Rn. 2; siehe dazu: Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/04/FAQ-zu-Cookies-und-Tracking.pdf; Bayerische Landesbeauftragte für den Datenschutz, abrufbar unter: https://www.datenschutz-bayern.de/6/SocialPlugins.html; Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, abrufbar unter: https://www.datenschutz.rlp.de/de/themenfelder-themen/webseiten-plugins.

37 *Rücker/Brandt* in Bräutigam/Rücker, E-Commerce, 1. Auflage 2017, D. Rn. 229.

38 *Rücker/Brandt* in Bräutigam/Rücker, E-Commerce, 1. Auflage 2017, D. Rn. 230.

39 Weiterführend: *Fuhlrott/Oltmanns*, NZA 2016, 785 ff.

40 Dies sind einerseits die personenbezogenen Daten des Mitarbeiters, der den Beitrag geschrieben hat (für dessen Verarbeitung regelmäßig eine Rechtsgrundlage vorliegen wird), andererseits aber auch personenbezogene Daten, die im Beitrag selbst erwähnt sind.

chende Verantwortlichkeit – inklusive Haftung und Risiken – ausreichen. In der Konsequenz müssten dann Arbeitgeber und Mitarbeiter – vielleicht im Rahmen des Arbeitsvertrages – Joint-Controllership-Vereinbarungen abschließen. Hier bleibt abzuwarten, wie sich die Rechtsprechung entwickelt und ob sich tatsächlich eine solch weite Interpretation durchsetzt.

III. Herausgabeanspruch von Daten

Häufig richten Mitarbeiter, die für den Auftritt des Arbeitgebers im Social Media Bereich verantwortlich sind, entsprechende Accounts auf ihren eigenen Namen ein, da dies mitunter schlicht einfacher ist. Hier sollte der Arbeitgeber entweder ein solches Vorgehen direkt verbieten oder durch geeignete Abreden sicherstellen, dass er bei einem Ausscheiden des Mitarbeiters vollen Zugriff auf diesen Account erlangt bzw. die Daten herausverlangen kann. Voraussetzung wird regelmäßig sein, dass es sich um einen rein geschäftlichen Account handelt und der Arbeitgeber dies auch nachweisen kann – dies kann in der Praxis schwierig werden, so dass sich ein Verbot empfiehlt.[41]

IV. Empfehlung: Social Media Guidelines

Auch wenn der Arbeitgeber den Mitarbeitern bei der Nutzung von privaten Netzwerken wenig bis gar keine Vorgaben machen kann, sollten diese zur Minimierung von Risiken im Umgang mit unternehmensbezogenen Inhalten bzw. berufsbezogenen Netzwerken durch Seminare und entsprechende Social Media Guidelines geschult werden.

Social Media Guidelines sind letztlich Handlungsempfehlungen für eine Kommunikation im Internet, die das Bewusstsein der Mitarbeiter für einen angemessenen Umgang mit Social Media sensibilisieren sollen. Die Guidelines können als Ergänzung des Arbeitsvertrages oder als Betriebsvereinbarung ausgestaltet sein. Darin sollten verschiedene Aspekte, wie die Trennung von privaten und beruflichen Aussagen, der Umfang der Nutzung von sozialen Netzwerken am Arbeitsplatz und Hinweise zu einer datenschutz- und urheberrechtskonformen Nutzung von Social Media geregelt werden. Zudem sollten die Mitarbeiter in den Social Media Guidelines darauf hingewiesen werden, dass für eine positive Außendarstellung des Unternehmens und des Mitarbeiters selbst ein respektvoller und rechtmäßiger Umgang mit Kollegen, Kunden und Wettbewerbern geboten ist.[42]

Wichtig ist, dass Social Media Guidelines empfehlenden und verbindlichen Charakter haben. Dafür, dass sie verbindlich sind, muss der Betriebsrat – falls vorhanden – beteiligt werden. Neben der Verbindlichkeit sind auch die Rechtsfolgen bei Missachtung der Regelungen zu nennen, und die Guidelines sind nachweislich durch den Mitarbeiter zur Kenntnis zu nehmen.[43]

E Fazit

Die Nutzung von Social Media bietet für Unternehmen enorme Chancen, sich selbst und die eigenen Produkte einem großen Publikum mit relativ geringem Aufwand bekannt zu machen. Jedoch liegen in dieser Möglichkeit auch zahlreiche Risiken, die sich allerdings durch die Umsetzung bestimmter Maßnahmen zumindest minimieren lassen. Unternehmen sollten insbesondere folgende Punkte berücksichtigen:

- Ist mit dem jeweiligen Anbieter der Social Media Plattform oder des Social Plugins eine Joint-Controller-Vereinbarung nach Art. 26 DSGVO abgeschlossen?
- Ist eine umfassende Datenschutzerklärung, gegebenenfalls durch eine Verlinkung, nebst Impressum des jeweiligen Betreibers z. B. einer Fanpage abrufbar?
- Wird auch über eingesetzte Social Plugins in der Datenschutzerklärung umfassend belehrt?
- Ist sichergestellt, dass eine Rechtsgrundlage den Austausch der Daten mit dem Anbieter erlaubt?
- Sofern bei Social PlugIns Einwilligungen eingeholt werden: Werden rechtskonforme Lösungen zu deren Nutzung (z. B. die Zwei-Klick-Lösung) eingesetzt?

Zudem sollten die Mitarbeiter – nicht nur diejenigen, die für den Betrieb der Unternehmensseite intern zuständig sind, sondern alle – durch Seminare oder Social Media Guidelines geschult werden. Arbeitgeber sollten sich immer Zugriff auf die bei dem Einsatz von Social Media im Unternehmen genutzten Accounts sichern. Zu guter Letzt sollte (neben den aktuellen Verlautbarungen der Datenschutzaufsichtsbehörden und der Rechtsprechung insbesondere des EuGH) auch die Entwicklung der E-Privacy-Verordnung[44] der EU verfolgt werden – hier ist für 2020 eine völlige Neuordnung des Online-Bereichs zu erwarten, der mit Sicherheit auch Neuerungen im Bereich Social Media mit sich führen wird.

41 Siehe auch: *Hoffmann-Remy*, NZA 2016, 792.

42 *Solmecke* in Hoeren/Sieber/Holznagel, Multimediarecht, Februar 2019, Teil 21.1 Rn. 82, 83.

43 *Solmecke* in Hoeren/Sieber/Holznagel, Multimediarecht, Februar 2019, Teil 21.1 Rn. 84.

44 Entwurf abrufbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52017PC0010.

Silvia C. Bauer ist Rechtsanwältin und Partnerin der Luther Rechtsanwaltsgesellschaft mbH. Ihre Tätigkeitsschwerpunkte sind das Datenschutzrecht sowie datenschutzrechtliche Compliance. Sie ist als externe Datenschutzbeauftragte sowie Konzerndatenschutzbeauftragte bei diversen Unternehmen bestellt und führt auf nationaler und europäischer Ebene Datenschutzaudits durch.

Kata Viktoria Eles ist als wissenschaftliche Mitarbeiterin bei der Luther Rechtsanwaltsgesellschaft mbH am Standort Köln tätig. Sie unterstützt dort den Bereich IP/IT und befasst sich im Schwerpunkt mit Datenschutz- und IT-Recht.