datenschutz-berater.de

45. Jahrgang DSB 05/2021

DATENSCHUTZ-BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

ISSN 0170-7256

dfv Mediengruppe

Stefan Hessel und Maximilian Leicht

Facebook, Twitter & Co. – Risiken für Unternehmen bei gemeinsamer Verantwortlichkeit

Soziale Netzwerke – wie Facebook, Twitter oder LinkedIn – sind für die Tätigkeit vieler Unternehmen alltäglich oder sogar essenziell. Insbesondere im Recruiting, Marketing oder in der Kundenkommunikation kann oft nicht ohne weitreichende Auswirkungen auf die Nutzung von sozialen Netzwerken verzichtet werden. Gleichzeitig sind damit für Unternehmen datenschutzrechtliche Risiken verbunden. Nach der weitreichenden EuGH-Rechtsprechung zu Art. 26 DSGVO bedeuten die gemeinsame Verantwortlichkeit und die damit verbundenen Rechtsfolgen für Unternehmen große Herausforderungen. Der Beitrag fokussiert die Risiken einer gemeinsamen Verantwortlichkeit für Unternehmen bei der Nutzung von sozialen Netzwerken und gibt Handlungsempfehlungen zur Risikominimierung.

Die Bedeutung der gemeinsamen Verantwortlichkeit bei sozialen Netzwerken

Ob im Recruiting, Marketing oder in der Kundenkommunikation: für Unternehmen sind soziale Netzwerke von enormer Bedeutung und aus dem täglichen Geschäft nicht mehr wegzudenken. Gleichzeitig bemängeln einige europäische Datenschutzaufsichtsbehörden, aber auch Verbraucherverbände und zivilgesellschaftliche Organisationen, insbesondere bei sozialen Netzwerken aus den USA, einen unzureichenden Datenschutz. Trotz der vehementen Äußerungen und mehrerer Gerichtsverfahren haben die Kritiker in den vergangenen Jahren gegenüber den Betreibern der Netzwerke kaum Verbesserungen durchsetzen können.

Die Gründe hierfür sind u. a. in der bisherigen Praxis der irischen Datenschutzaufsicht zu verorten, welche hinsichtlich der sozialen Netzwerke eine große Zurückhaltung walten lässt. Trotz entsprechend deutlicher und auch öffentlichkeitswirksamer Kritik am Verhalten der Aufsichtsbehörde – wie sie etwa zuletzt mehrfach vom BfDI geäußert wurde – lassen sich bisher jedoch keine wesentlichen Veränderungen feststellen. Wegen dieser Patt-Situation, geraten spätestens seit dem EuGH-Urteil zu Facebook-Fanpages (EuGH, Urt. v. 05.06.2018 – C-210/16) und dem darauf folgenden Urteil des BVerwG vom (BVerwG, Urt. v. 11.09.2019 – 6 C 15.18) verstärkt Unternehmen und andere Nutzer der Netzwerke, die sich nicht auf die Haushaltsausnahme des Art. 2 Abs. 2 lit. c DSGVO berufen können, ins Fadenkreuz der Kritiker. Diese Entscheidungen – wie auch die anderen in diesem Beitrag angesprochenen EuGH-Urteile – beziehen sich auf die RL 95/46/EG, sind jedoch auf die DSGVO übertragbar (siehe Lang, DSB 2019, 206 f.). Die bisherige Rechtsprechung des EuGH legt den Begriff der gemeinsamen Verantwortlichkeit weit aus. Dadurch werden die Unternehmen und die Netzwerkbetreiber tendenziell gleichermaßen zur Einhaltung des Datenschutzrechts verpflichtet – was es den Kritikern der Netzwerke grundsätzlich ermöglichen kann, ihre Rechtsauffassung auch gegenüber den Unternehmen durchzusetzen.

Rechtlicher Hintergrund

Als Basis der folgenden Risikobewertung wird zunächst der Tatbestand des Art. 26 DSGVO sowie die zugehörige Rechtsprechung des EuGH erläutert.

Der Tatbestand der gemeinsamen Verantwortlichkeit

Eine gemeinsame Verantwortlichkeit setzt nach Art. 26 Abs. 1 Satz 1 DSGVO voraus, dass zwei oder mehr Verantwortliche gemeinsam eine Entscheidung über Zwecke und Mittel der Verarbeitung treffen. Die gemeinsame Entscheidung über Zwecke und Mittel ist zugleich das wichtigste Abgrenzungskriterium gegenüber der Auftragsverarbeitung gem. Art. 28 DSGVO. Der Auftragsverarbeiter wird nämlich ausschließlich als Hilfsperson und auf Weisung des Verantwortlichen tätig und darf insofern zwar in einem gewissen Umfang über die Mittel der Verarbeitung entscheiden, jedoch keinesfalls über ihre Zwecke. Verfolgt der Auftragsverarbeiter bei einer Datenverarbeitung nicht mehr ausschließlich die Interessen des Verantwortlichen, sondern darüber hinaus auch eigene Interessen, liegt daher keine Auftragsverarbeitung mehr vor.

Im Fall einer gemeinsamen Verantwortlichkeit müssen die beteiligten Verantwortlichen die Entscheidung über die Zwecke und Mittel der Verarbeitung gemeinsam treffen. Ist dies nicht der Fall, liegt keine gemeinsame Verantwortlichkeit vor, sondern eine Datenübermittlung zwischen zwei eigenständig Verantwortlichen („controller-to-controller“). Die Messlatte für eine gemeinsame Entscheidung ist allerdings nicht sehr hoch. Eine gemeinsame Verantwortlichkeit kommt daher nach der Rechtsprechung des EuGH auch in Betracht, wenn zwei oder mehr Verantwortliche unterschiedlich stark oder auf unterschiedliche Weise an der Festlegung von Zwecken und Mitteln beteiligt sind. Maßgeblicher Anknüpfungspunkt für die gemeinsame Entscheidung ist – wie der EuGH in seinem „Fashion ID”-Urteil (EuGH, Urt. v. 29.07.2019 – C-40/17) klargestellt hat – die einzelne Verarbeitungsphase. Es kann also eine gemeinsame Entscheidung über die Zwecke und Mittel einer

Datenverarbeitung vorliegen, obwohl weitere anschließende Verarbeitungsphasen von den beteiligten Verantwortlichen in einzelner Verantwortlichkeit durchgeführt werden.

Ausreichend ist damit – wie das „Zeugen Jehovas-Urteil" des EuGH (EuGH, Urt. v. 10.07.2018 – C-25/17) zeigt – letztlich jede Form des kumulativen Zusammenwirkens bei Datenverarbeitungen, soweit eine Mitentscheidung über die Zielrichtung und Modalitäten der Verarbeitung vorliegt. Besteht eine gemeinsame Verantwortlichkeit, verpflichtet Art. 26 Abs. 1 Satz 2 DSGVO die gemeinsam Verantwortlichen in transparenter Form festzulegen, wer von ihnen welche Verpflichtungen der DSGVO erfüllt. Die Vereinbarung hat jedoch keine konstitutive Wirkung. Ihr Fehlen führt folglich nicht zu einer Nichtigkeit oder dem Nichtvorliegen einer gemeinsamen Verantwortlichkeit.

Die Fanpage-Entscheidung des EuGH

Für den Kontext der sozialen Medien ist primär die Fanpage-Entscheidung des EuGH relevant. In dieser stellte das Gericht fest, dass zwar die bloße Nutzung von Facebook – ohne dabei eine Fanpage zu betreiben – nicht für eine gemeinsame Verantwortlichkeit mit dem sozialen Netzwerk ausreichen soll. Durch das Betreiben einer Fanpage ergebe sich jedoch eine andere Bewertung. Seitenbetreiber sind nach dem EuGH an der Entscheidung über die Zwecke und Mittel der Datenverarbeitung beteiligt. Den Betreibern werden von Facebook Besucherstatistiken bezüglich der Fanpages bereitgestellt. Zwar geschieht dies ausschließlich in anonymisierter Form. Dem vorhergehend ist allerdings das Abspeichern von Cookies durch Facebook auf den Endgeräten der Seitenbesucher sowie die nachfolgende Verarbeitung für statistische Zwecke eine Verarbeitung von personenbezogenen Daten. Dies gilt ebenso für die Möglichkeiten des Seitenbetreibers, diese Statistiken zu parametrieren – auch wenn diese Möglichkeiten durch den Betreiber nicht genutzt werden.

Daneben stellt der EuGH in der Entscheidung fest, dass es für eine gemeinsame Verantwortlichkeit gerade keiner gleichwertigen Verantwortlichkeit bedarf. Vielmehr sei ein Einbezug „in verschiedene Phasen und unterschiedlichem Ausmaß" denkbar, sodass der „Grad der Verantwortlichkeit" jeweils „unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen ist" (Rn. 43). Es sei daneben für eine Annahme einer gemeinsamen Verantwortlichkeit nicht erforderlich, dass alle Verantwortlichen Zugriff auf die verarbeiteten Daten haben.

Der EuGH betont zugleich die Prüfung des jeweiligen Einzelfalls und lässt eine bloße Nutzung von Facebook nicht für eine gemeinsame Verantwortlichkeit ausreichen. Hieraus ist zu schließen, dass selbst im Bereich von sozialen Netzwerken nicht ohne Weiteres und in jedem Fall eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO vorliegen wird. Insbesondere müssten die jeweiligen Nutzerkonten bei anderen Netzwerken eine der Parametrierung oder Verarbeitung von Cookies rechtlich vergleichbare Funktionalität aufweisen. Hierfür ist eine jeweilige Prüfung im Einzelfall notwendig, die insbesondere auch die technischen Hintergründe der Auswertungsmöglichkeiten betrachtet und – bei der üblichen regelmäßigen Veränderung durch Weiterentwicklungen und Updates – auch einer dynamischen rechtlichen Betrachtung unterliegen muss. Dem Fanpage-Urteil ist insofern keine allgemein für alle soziale Netzwerke abschließende Beurteilung der Verantwortlichkeit zu entnehmen.

Kriterien für eine gemeinsame Verantwortlichkeit in sozialen Netzwerken

Grundsätzlich ist bei der Prüfung einer gemeinsamen Verantwortlichkeit zunächst zu evaluieren, ob die jeweilige Stelle in Bezug auf die vorgenommene Verarbeitung überhaupt Verantwortlicher oder ggf. nur Auftragsverarbeiter ist. Für entsprechende Abgrenzungskriterien kann beispielsweise auf die Leitlinien des EDSB verwiesen werden (EDSB, Guidelines 2018/1725, 07.11.2019, S. 14 f. und S. 23). Bei den derzeit größten sozialen Netzwerken wird jedoch eine Verantwortlichkeit regelmäßig zu bejahen sein. Eine abweichende Bewertung ist insbesondere bei dezentralen oder unternehmensinternen sozialen Netzwerken denkbar, deren Betreiber nur im Auftrag des Unternehmens agieren.

Liegt eine Verantwortlichkeit vor, sollte in der Folge bewertet werden, ob auch eine gemeinsame Verantwortlichkeit mit dem Netzwerk vorliegt. Hierfür sind zwei Kriterien maßgeblich.

Kriterium 1: Beteiligung an der Entscheidung über die Mittel der Datenverarbeitung

Relevant ist zunächst, ob das Unternehmen tatsächlich an der Entscheidung über die Mittel der Datenverarbeitung beteiligt ist. Daran sind nach der EuGH-Rechtsprechung grundsätzlich keine allzu hohen Voraussetzungen anzulegen. Vielmehr sollen bereits geringe Möglichkeiten der Einflussnahme ausreichen. Insbesondere könne dies der Fall sein, wenn ohne Beteiligung des Unternehmens die personenbezogenen Daten schlicht nicht verarbeitet werden würden – etwa, weil die Fanpage nicht erstellt wird und die Daten daher nicht erhoben werden.

Fehlt eine gemeinsame Entscheidung über die Zwecke und Mittel der Verarbeitung bezüglich einzelner Vorgänge in einer Folge mehrerer Phasen der Verarbeitung, so besteht für diese keine gemeinsame Verantwortung (siehe Lang, DSB 2019, 206, 207 f.).

Für eine Beteiligung sprechen dabei u. a. Einwirkungsmöglichkeiten des Unternehmens auf die vom Betreiber vorge-

nommenen Datenverarbeitungen, etwa die Einstellung von Parametern, wie z. B.:

- die Auswahl und Eingrenzung von Nutzergruppen oder
- die Auswahl bzw. Eingrenzung von Datenkategorien.

Diese Einwirkungsmöglichkeiten sind besonders bei der Bereitstellung von (Besucher-)Statistiken und anderen Zugriffsdaten der Zielgruppe relevant.

Kriterium 2: Vergleich der jeweils und gemeinsam festgelegten Zwecke der Datenverarbeitung

Es sind auch die verfolgten Zwecke von Netzwerkbetreiber und Nutzer zu betrachten. Bei übereinstimmenden oder komplementären Zwecken liegt eine gemeinsame Verantwortlichkeit nahe. Hierfür ist nach dem EuGH unerheblich, ob beide Verantwortliche Zugang zu den personenbezogenen Daten haben. Eine gemeinsame Verantwortlichkeit kann daher auch vorliegen, wenn einer der Verantwortlichen die Daten (oder die Ergebnisse der Verarbeitung) nur in anonymisierter Form erhält. Eine Wahrnehmung gleichgelagerter (wirtschaftlicher) – und damit komplementärer – Interessen nimmt der EuGH etwa an, wenn der Nutzer aggregierte Auswertungen erhält. Dies gilt jedenfalls dann, wenn die Auswertungen für ihn wirtschaftlich vorteilhaft sind und zugleich das soziale Netzwerk – im Rahmen des zugrunde liegenden Geschäftsmodells – die hierfür erhobenen personenbezogenen Daten auch zu eigenen Zwecken verarbeitet. Solche Statistiken sind in der Praxis üblich und können es dem Nutzer ermöglichen, seine Social-Media-Präsenz zur besseren Vermarktung zu optimieren. Hierfür stellen die sozialen Netzwerke bspw. Zugriffszahlen sowie verschiedene Interaktionsraten bereit und heben hervor, welche Beiträge des Fanpage-Inhabers besonders erfolgreich waren.

Daneben sind aber auch weitere Szenarien denkbar, in denen zwischen Fanpage-Inhaber und Netzwerkbetreiber komplementäre Zwecke vorliegen. Dies kann etwa der Fall sein, wenn Verantwortliche über das soziale Netzwerk personenbezogene Daten Dritter verarbeiten, etwa aufgrund einer Kommunikation mit oder über Kunden des Verantwortlichen.

Übertragbarkeit der Entscheidung auf andere soziale Netzwerke

Die folgende Tabelle enthält eine erste Hilfestellung zur individuellen Prüfung durch Unternehmen, inwieweit die erläuterten Kriterien – abhängig vom konkreten Nutzungsszenario – bei den genannten sozialen Netzwerken gegeben sein können. Relevant ist dabei, dass die Netzwerke überwiegend zwischen Nutzer-Accounts und professionellen Accounts unterscheiden. Damit ist auch ein Unterschied bei den angebotenen Statistiken verbunden. Für gewöhnliche Nutzer-Accounts ist daher ggf. eine andere Bewertung vorzunehmen. Tendenziell liegt – nach hier vertretener Ansicht – in so einem Fall keine gemeinsame Verantwortlichkeit vor. Außer Betracht bleibt bei der Einschätzung die Möglichkeit, Werbung im sozialen Netzwerk zu schalten. Für professionelle Konten bei Instagram ist anzumerken, dass die Vereinbarung zur gemeinsamen Verantwortlichkeit mit Facebook, der sogenannte „Zusatz für Verantwortliche", grundsätzlich die Möglichkeit für eine Übertragung auf Instagram bietet. Allerdings existiert mit Stand vom 25.04.2021 keine entsprechende Bezugnahme in den Instagram-Nutzungsbedingungen, wie sie etwa für Facebook-Fanpages oder die Facebook Business-Tools vorhanden ist.

Soziales Netzwerk	Kriterium 1: Entscheidung über die Mittel	Kriterium 2: Festlegung der Zwecke	Vereinbarung nach Art. 26 DSGVO vorhanden?
Facebook-Fanpage	Ja	Ja	Ja
Twitter	Nein	Strittig	Nein
Instagram (professionelles Konto)	Ja	Ja	Nein
XING (Arbeitgeberprofil)	Ja	Ja	Nein
LinkedIn (Unternehmensseite)	Ja	Ja	Ja
LinkedIn (Unternehmensseite)	Ja	Ja	Ja
TikTok (Pro-Account)	Nein	Ja	Nein
Clubhouse	Nein	Strittig	Nein

Risiken für Verantwortliche und Maßnahmen zur Risikoreduzierung

Besteht bei sozialen Netzwerken eine gemeinsame Verantwortlichkeit, können sich hieraus erhebliche Risiken für Unternehmen ergeben. Diese können zunächst darin bestehen, dass die rechtliche Situation falsch bewertet wird und eine Auftragsverarbeitung oder eine getrennte statt einer gemeinsamen Verantwortlichkeit der Beteiligten angenommen wird. In diesen Fällen kann es bereits an der nach Art. 26 Abs. 1 Satz 2 DSGVO erforderlichen Vereinbarung zur gemeinsamen Verantwortlichkeit fehlen, was nach Art. 83 Abs. 4 lit. a DSGVO bußgeldbewehrt sein kann. Davon losgelöst sind Unternehmen bei einer gemeinsamen Verantwortlichkeit mit einem sozialen Netzwerk auch

selbst Adressat datenschutzrechtlicher Verpflichtungen. Die Unternehmen sind – jedenfalls soweit sie einen Beitrag zur Entscheidung über die Zwecke und Mittel leisten – dem Betreiber des sozialen Netzwerks gleichgestellt und gleichsam zur Einhaltung des Datenschutzrechts verpflichtet. Besonders kritisch ist diese Konstellation, wenn der Betreiber des sozialen Netzwerks und das Unternehmen sich in unterschiedlichen EU-Mitgliedstaaten befinden und folglich der Aufsicht anderer Behörden unterliegen. Trotz der durch die DSGVO angestrebten Vollharmonisierung des Datenschutzrechts kann es nämlich – wie beispielsweise der Vergleich zwischen den Anforderungen der Datenschutzaufsicht in Deutschland und Irland zeigt – zu unterschiedlichen Auslegungen der DSGVO, aber auch zu einer abweichenden Praxis bei der Durchsetzung kommen. Nicht zu vernachlässigen ist auch, dass die Nutzung eines sozialen Netzwerks der Natur der Sache nach öffentlich stattfindet und tatsächliche oder vermeintliche Verstöße daher durch ein breites Publikum festgestellt werden können. Daher bleibt das Risiko für Unternehmen insgesamt hoch, auch wenn die gemeinsame Verantwortlichkeit bei sozialen Netzwerken derzeit bei den Datenschutzaufsichtsbehörden etwas aus dem Fokus gerückt zu sein scheint.

Grundsätzlich ist Unternehmen daher zu raten, vor der Nutzung eines sozialen Netzwerks eine Risikoanalyse durchführen, diese zu dokumentieren und bei Bedarf risikominimierende Maßnahmen zu ergreifen. Im Zentrum der Risikoanalyse sollte dabei die Frage stehen, inwieweit die Entscheidung des EuGH zu Facebook-Fanpages auf das jeweilige soziale Netzwerke übertragbar ist. Neben der Bewertung durch das soziale Netzwerk sollten dabei außerdem etwaige Verlautbarungen und Stellungnahmen der Datenschutzaufsichtsbehörden einbezogen werden. Auch ein vorheriges Gespräch mit der zuständigen Aufsichtsbehörde kann in diesem Kontext sinnvoll sein.

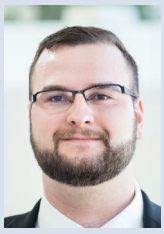
Kommt die Analyse zum Ergebnis, dass eine gemeinsame Verantwortlichkeit besteht, ist zu prüfen, ob der Betreiber die Möglichkeit bietet, eine entsprechende Vereinbarung zu treffen. Ist dies der Fall, ist es in der Regel ratsam, die Vereinbarung nach einer rechtlichen Prüfung abzuschließen. Darüber hinaus sollten Unternehmen das Ergebnis der Risikoanalyse regelmäßig überprüfen und dabei neue Risikofaktoren – wie allgemeine Prüfverfahren der Aufsichtsbehörden oder eingeleitete Verfahren gegen andere Unternehmen oder den Betreiber des sozialen Netzwerkes – berücksichtigen. Solche Prüfverfahren werden aktuell bspw. durch die Berliner Datenschutzaufsicht durchgeführt (BlnBDI, Tätigkeitsbericht für das Jahr 2020, S. 203-205). Ein guter Indikator ist in diesem Zusammenhang auch die Nutzung entsprechender Netzwerke durch die Aufsichtsbehörden selbst oder durch andere öffentliche Stellen. Intern sollten Unternehmen darüber hinaus Nutzungskonzepte aufstellen, die insbesondere eine interne Kommunikation zwischen Beschäftigten und die Verarbeitung sensibler Daten über das soziale Netzwerk verbieten sollten.

Fazit und Ausblick

Zusammenfassend kann festgehalten werden, dass die vom EuGH aufgestellten Kriterien zur Beurteilung einer gemeinsamen Verantwortlichkeit bei Facebook-Fanpages wegen ihrer Unbestimmtheit nur schwer auf andere soziale Netzwerke übertragbar sind. Mit Blick darauf, dass der EuGH in seiner bisherigen Rechtsprechung jedoch eher durch eine ausufernde Interpretation der Maßstäbe für eine gemeinsame Verantwortlichkeit aufgefallen ist, dürfte bei vielen sozialen Netzwerken davon auszugehen sein, dass Art. 26 Abs. 1 DSGVO einschlägig ist. Unternehmen, die auf den Einsatz sozialer Netzwerke aus wirtschaftlichen Gründen angewiesen sind, können daher schnell zum Spielball in einem Konflikt um die datenschutzrechtlichen Anforderungen an die Netzwerkbetreiber werden.

Aus Unternehmenssicht sind daher eine fortlaufende Risikoanalyse und Dokumentation sowie erforderlichenfalls risikominimierende Maßnahmen notwendig. Darüber hinaus wäre es zu begrüßen, wenn sich die europäischen Aufsichtsbehörden auf eine einheitliche Bewertung und Durchsetzungspraxis einigen würden. Für Verantwortliche dürfte es gleichzeitig erfreulich sein, dass die Datenschutzaufsicht Bremen in ihrem aktuellen Tätigkeitsbericht für das Jahr 2020 (dort S. 56) davon auszugehen scheint, dass ein Fanpage-Betreiber im Falle eines Auskunftsersuchens durch einen Betroffenen mit der Weiterleitung des Begehrens an Facebook seinen insoweit bestehenden datenschutzrechtlichen Verpflichtungen nachgekommen ist.

Autoren: **Stefan Hessel ist Rechtsanwalt und Associate im Team Cybersecurity & Datenschutz bei reuschlaw Legal Consultants in Saarbrücken.**



Maximilian Leicht ist wissenschaftlicher Mitarbeiter und Doktorand am Lehrstuhl für Rechtsinformatik (Prof. Dr.-Ing. Christoph Sorge) der Universität des Saarlandes.