Datenschutz im Internet

Schwartmann / Benedikt / Reif

2025
ISBN 978-3-406-78340-1
C.H.BECK

inhalts auf einem beliebigen Erklärungsträger.[62] Ein Ausdruck ist nicht erforderlich und insbesondere braucht die elektronische Form iSv § 126a BGB, die eine qualifizierte elektronische Signatur voraussetzt, nicht eingehalten zu werden.[63] Gleichwohl genügt nicht jegliche elektronische Form den Anforderungen nach Art. 28 Abs. 9 DS-GVO.[64] Denn es muss nachvollziehbar sein, dass die Vertragsparteien, die in dem Dokument genannt sind, sich tatsächlich zu den eingegangenen Verpflichtungen mit dem konkreten Inhalt bekannt haben, was im Fall des Vertragsschlusses per E-Mail **regelmäßig zumindest** eine **einfache elektronische Signatur** voraussetzt.[65] Nach dem BayLDA genügt auch der nachweisbare Versand der unterschriebenen und eingescannten Vertragsdokumente per E-Mail.[66]

Hinsichtlich der **Regelung der Auftragsverarbeitung** sind diverse **Muster** verfügbar, an denen sich die Parteien orientieren können.[67] Auch einige Datenschutzaufsichtsbehörden haben entsprechende Mustervereinbarungen veröffentlicht.[68] Seit 2021 existieren zudem Standardvertragsklauseln der EU-Kommission für die Auftragsverarbeitung.[69] 37

Bei den in Art. 28 Abs. 3 S. 2 DS-GVO enthaltenen inhaltlichen Vorgaben an den Auftragsverarbeitungsvertrag handelt es sich nur um **Mindestanforderungen.** Zusätzliche Regelungen können ratsam sein, zB zu Haftungs- oder Vergütungsfragen, wobei Letztere typischerweise im Hauptvertrag geregelt werden. Eine Bezugnahme auf den hinter dem Auftragsverarbeitungsvertrag stehenden zivilrechtlichen Hauptvertrag ist auch bezüglich der Regelungsinhalte nach Art. 28 Abs. 3 S. 2 DS-GVO zulässig und sinnvoll, solange der Hauptvertrag hinreichend spezifische und konkrete Einzelangaben zu den angeführten Punkten enthält.[70] 38

Eine praxisrelevante Frage im Zusammenhang mit der Vergütung besteht darin, ob ein **gesondertes Entgelt für Kontrollen** des Verantwortlichen vorgesehen werden darf. Der EDSA[71] führt insoweit aus, dass die Frage der Kostenverteilung zwischen einem Verantwortlichen und einem Auftragsverarbeiter im Zusammenhang mit Überprüfungen im Grundsatz nicht der DS-GVO unterfällt, sondern wirtschaftlichen Erwägungen unterliegt. Die Vertragsparteien sollten aber keine Klauseln vereinbaren, welche die Zahlung eindeutig unangemessener oder unverhältnismäßig hoher Kosten und Gebühren für Kontrollen zum Gegenstand haben und daher abschreckende Wirkung haben, so der EDSA. Ansonsten bestünde die Gefahr, dass Rechte, die integraler Bestandteil der Datenschutzgarantien nach Art. 28 DS-GVO sind, faktisch nicht ausgeübt werden. 39

b) Einsatz von Subunternehmen. Art. 28 DS-GVO gestattet es grundsätzlich auch, dass der Auftragsverarbeiter sich zur Erbringung der geschuldeten Dienstleistung eines weiteren Auftragsverarbeiters bedient, also Subunternehmer einsetzt, sofern **zwei Voraussetzungen** erfüllt sind: Die Einschaltung von Subunternehmern durch den Auftragsverarbeiter 40

[62] Schwartmann/Jaspers/Thüsing/Kugelmann/Kremer DS-GVO Art. 28 Rn. 178.
[63] Paal/Pauly/Martini DS-GVO Art. 28 Rn. 75.
[64] Paal/Pauly/Martini DS-GVO Art. 28 Rn. 75.
[65] Müthlein RDV 2016, 74 (76).
[66] BayLDA, FAQ zur DS-GVO, 19.7.2018, www.lda.bayern.de/media/FAQ_ADV_Formerfordernis.pdf.
[67] Vgl. etwa bitkom, Mustervertragsanlage Auftragsverarbeitung iSd Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO), Version 1.2 2023; GDD, Praxishilfe DS-GVO: Mustervertrag zur Auftragsverarbeitung nach Art. 28 DS-GVO, Version 2.1 Juni 2021, auch in engl. Sprache verfügbar.
[68] So etwa LfD Nds., BayLDA und LfD BW (zur aktuellen Version der Dokumente vgl. die jew. Webseiten der Aufsichtsbehörden).
[69] Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates (ABl. 2021 L 199, 18).
[70] Koreng/Lachenmann DatenschutzR-FormHdB/Schmidt/Brink Form. G.I.4. Anm. 8.
[71] EDSA, Leitlinien 7/2020 Rn. 145; zum Ganzen auch BayLfD, Aktuelle Kurz-Information 6: Entgeltpflicht für Kontrollen bei der Auftragsverarbeitung?, 15.11.2021.

kommt nach Art. 28 Abs. 2 DS-GVO nur bei **vorheriger Genehmigung durch den Verantwortlichen** in Betracht, wobei die Regelung zwei verschiedene Lösungen zur Erteilung der Genehmigung vorsieht. Möglich ist eine spezifische vorherige Genehmigung bezogen auf einen konkreten Subunternehmer (Genehmigung im engeren Sinne). Es kann aber auch im Vorfeld eine allgemeine schriftliche Genehmigung zum Subunternehmereinsatz erteilt werden. In letzterem Fall informiert der Auftragsverarbeiter den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragnehmern, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Diese Lösung wird daher auch als „Einspruchslösung" bezeichnet. Zudem muss gewährleistet werden, dass der **Vertrag des Auftragsverarbeiters mit dem Subunternehmer** inhaltlich die **gleichen Pflichten** vorsieht, wie sie der Auftragnehmer selbst zugunsten des Auftraggebers übernommen hat, die Pflichten aus dem Ausgangsvertrag müssen also entsprechend durchgereicht werden (Art. 28 Abs. 4 S. 1 DS-GVO). Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, **so haftet** insoweit **der erste Auftragsverarbeiter** gegenüber dem Verantwortlichen (Art. 28 Abs. 4 S. 2 DS-GVO). Die in Art. 28 Abs. 2, 4 DS-GVO genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters gehören nach Art. 28 Abs. 3 S. 2 lit. d DS-GVO auch zu den notwendigen **Pflichtinhalten des Auftragsverarbeitungsvertrages.**

41 Die Einschaltung von Subunternehmen ist in der Praxis vor allem mit **tatsächlichen Herausforderungen** verbunden, die sich daraus ergeben, als Auftraggeber überhaupt einen Überblick zu erlangen und – angesichts des beständigen Wechsels der Geschäftsbeziehungen durch Unternehmen – auch zu behalten, welche Subunternehmen konkret im Rahmen der vergebenen Aufträge tätig werden. So entwickeln etwa viele „Software as a Service (SaaS)"-Anbieter lediglich die Software, betreiben aber keine eigenen Rechenzentren, sondern kaufen Hosting-Leistungen ihrerseits von Drittanbietern ein.[72] Zudem wird SaaS auch von Zwischenhändlern angeboten, welche die Leistungen ihrerseits beim Softwarehersteller einkaufen.[73] Hierdurch entstehen Ketten von Subunternehmern, was Probleme nicht nur datenschutzrechtlicher Natur, sondern zB auch dann begründet, wenn im Rahmen der Erbringung der Dienstleistung Fehler auftreten.[74] Die (Gesamt-)Übersicht der leistenden Unterauftragnehmer sollte stets aktuell gehalten werden.[75] Mit der Zahl der Subunternehmer erhöhen sich aus Sicht des Auftraggebers regelmäßig die Risiken des Gesamtvertrages.[76]

42 Noch gesteigert würden die dargestellten Herausforderungen, sofern man annähme, dass der Hauptauftraggeber auch für die **sorgfältige Auswahl und Überwachung der Subauftragnehmer** zuständig ist. Hiergegen wird zu Recht eingewandt, dass ein unmittelbarer Zugriff des Auftraggebers auf die Unterauftragsverarbeiter zB beim Cloud Computing schwierig umzusetzen ist und faktisch in der Regel nicht zustande kommt.[77] Für die Überwachung des Subunternehmers durch den Auftragsverarbeiter spricht auch, dass Letzterer im Verhältnis zu seinem Auftraggeber haftet, wenn der Subunternehmer Datenschutzpflichten nicht nachkommt. Insofern sollte der Auftragsverarbeiter auch zuständig für die Überwachung sein. Anders als der erste Auftraggeber hat er insoweit auch die korrelierenden zivilrechtlichen Druckmittel. Der Verantwortliche dagegen muss grundsätzlich nur seinen Auftragsverarbeiter kontrollieren und sich dabei vergewissern, dass dieser wiederum seiner Kontrollpflicht gegenüber den Unterauftragsverarbeitern nachkommt.[78] Eine Durchgriffsmöglichkeit des Hauptauftraggebers gegenüber dem Subunternehmer zu ver-

[72] Heydn MMR 2020, 435 (436).
[73] Heydn MMR 2020, 435 (436).
[74] Heydn MMR 2020, 435 (436).
[75] Koreng/Lachenmann DatenschutzR-FormHdB/Müller Form. G.II.1. Anm. 1.
[76] Koreng/Lachenmann DatenschutzR-FormHdB/Müller Form. G.II.1. Anm. 1.
[77] Müthlein RDV 2016, 74 (82); Kühling/Buchner/Hartung DS-GVO Art. 28 Rn. 86.
[78] Kühling/Buchner/Hartung DS-GVO Art. 28 Rn. 86.

einbaren, kann ggf. ratsam sein für den Fall, dass Zweifel an der Aufsicht durch den Auftragsverarbeiter auftauchen.[79] Nach Ansicht des EDSA sollte der Auftraggeber im Fall einer allgemeinen Genehmigung zur Inanspruchnahme von Unterauftragsverarbeitern im Übrigen Richtkriterien im Hinblick auf die Auswahl der Subunternehmer vorgeben, zB Garantien in Bezug auf technische und organisatorische Maßnahmen, Fachwissen, Zuverlässigkeit und Ressourcen.[80] Dies ergebe sich aus dem Grundsatz der Rechenschaftspflicht in Art. 24 DS-GVO und der Verpflichtung, den Bestimmungen von Art. 28 Abs. 1, Art. 32 und Kapitel V DS-GVO zu genügen, so der EDSA.

c) Auftragsverarbeitung trotz überlegener Marktmacht des Dienstleisters? Kaum von der Hand gewiesen werden kann, dass gerade im Zusammenhang mit der Nutzung von Onlinediensten in der Praxis vielfach eine überlegene Marktmacht der Anbieterseite besteht. Die Websitebetreiber sind auf Informationen zur Datenverarbeitung angewiesen, welche ihnen vom Diensteanbieter zur Verfügung gestellt werden, und sind oftmals nicht in der Position, Anforderungen an die Datenverarbeitung oder den Inhalt datenschutzrechtlicher Verträge bzw. Vereinbarungen zu stellen. Ausgeschlossen ist das Vorliegen einer Auftragsverarbeitung in solchen Fällen nicht. Es ist allerdings mit besonderer Sorgfalt zu prüfen, ob der marktmächtigere Auftragnehmer **tatsächlich rein weisungsgebunden** im Dienst des Auftraggebers tätig wird und sich dessen Aufsicht unterwirft oder ob der vermeintliche Auftragsverarbeiter nicht doch über Zwecke und/oder wesentliche Mittel der Verarbeitung (mit-)bestimmt. Die Situation ist vergleichbar denjenigen Fällen, in denen in Konzernstrukturen ein Tochterunternehmen die gesellschaftsrechtlich übergeordnete Muttergesellschaft als Auftragsverarbeiter einschaltet. Auch insoweit wird die pauschale Annahme einer Weisungsunfähigkeit der Konzerntochter überwiegend abgelehnt, da sich im Einzelfall durchaus auch die Konzernobergesellschaft Weisungen der untergeordneten Gesellschaften unterwerfen könne.[81] 43

Zu beachten ist zudem, dass das Problem entgegengesetzter Macht- und Einflussverhältnisse bei Onlinediensten durch die Ablehnung einer Auftragsverarbeitung auch nicht gelöst würde, sondern nur verschoben. Denn Alternative wäre die Annahme einer (gemeinsamen oder auch getrennten) datenschutzrechtlichen Verantwortlichkeit, obwohl angesichts des Machtgefälles hier ebenso zweifelhaft erscheint, inwiefern der Websitebetreiber tatsächlich auf Zwecke und Mittel der Datenverarbeitung Einfluss nehmen kann. 44

4. Rechtsfolgen und Haftung im Fall der Auftragsverarbeitung

Ein Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden, wenn er entweder seinen **speziell den Auftragsverarbeitern auferlegten Pflichten** aus der DS-GVO nicht nachgekommen ist oder er unter **Nichtbeachtung der** rechtmäßig **erteilten Anweisungen** des für die Datenverarbeitung Verantwortlichen bzw. gegen diese Anweisungen gehandelt hat (Art. 82 Abs. 2 S. 2 DS-GVO). Im Verhältnis zum Auftraggeber haftet der Auftragsverarbeiter gemäß Art. 82 Abs. 4 DS-GVO als **Gesamtschuldner.** Der Anspruchsberechtigte hat damit unabhängig vom Grad des Verschuldens und der jeweiligen Finanzkraft grundsätzlich die freie Wahl, von welchem Anspruchsgegner er den Schaden ersetzt haben möchte. Im Innenverhältnis zwischen Verantwortlichem und Auftragsverarbeiter erfolgt ein Ausgleich unter Berücksichtigung der jeweiligen Verantwortungsbeiträge (Art. 82 Abs. 5 DS-GVO). 45

Wie der Verantwortliche hat auch der Auftragsverarbeiter gemäß Art. 82 Abs. 3 DS-GVO die Möglichkeit sich **von der Haftung** zu **befreien,** indem er nachweist, dass er in 46

[79] Borges/Meents Cloud Computing/Borges § 7 Rn. 132.
[80] EDSA, Leitlinien 7/2020 Rn. 156.
[81] Vgl. etwa von dem Bussche/Voigt Konzerndatenschutz/Voigt Teil 3. Kap. 5 Rn. 3; Kühling/Buchner/Hartung DS-GVO Art. 28 Rn. 55; Taeger/Gabel/Gabel/Lutz DS-GVO Art. 28 Rn. 23; Petri ZD 2015, 305 (307).

keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist **(Exkulpation).**[82]

47 Nicht nur als Auftragsverarbeiter, sondern als Verantwortlicher haftet ein Dienstleister im **Fall des Exzesses,** also, wenn er unter Verstoß gegen die DS-GVO Zwecke und Mittel der Verarbeitung bestimmt, vgl. Art. 28 Abs. 10 DS-GVO. In diesem Fall ist der Auftragsverarbeiter außerdem den erweiterten Bußgeldtatbeständen für Verantwortliche ausgesetzt[83] und kann etwa Adressat eines Bußgeldbescheids wegen unzulässiger Datenverarbeitung sein.

48 Außerhalb von Exzesskonstellationen kommen **Bußgelder nach Art. 83 Abs. 4 lit. a DS-GVO** in Betracht, welcher unter anderem Verstöße gegen Art. 28 DS-GVO sanktioniert. Die genannte Bußgeldvorschrift erfasst Pflichtverletzungen von Verantwortlichen wie auch von Auftragsverarbeitern im Zusammenhang mit Art. 28 DS-GVO.

5. Beispiele für Auftragsverarbeitungen im Zusammenhang mit Onlineangeboten

49 Praxisbeispiel für eine Auftragsverarbeitung nach Art. 28 DS-GVO sind etwa **Webhosting**-Dienste. Entsprechende Anbieter bieten Websitebetreibern Webserver und damit Speicherplatz, damit deren Angebote überall auf der Welt rund um die Uhr erreichbar sind. Entsprechendes gilt für **Storage-as-a-Service-(STaaS)**-Lösungen, die cloudbasiert zur Verfügung gestellt werden. Auch **Software-as-a-Service-(SaaS)**-Angebote können über Art. 28 DS-GVO realisiert werden, vorausgesetzt, der SaaS-Dienstleister verwendet die Daten nicht auch für eigene Zwecke, zB für Auswertungen zum Zwecke der Qualitätssicherung oder Produktoptimierung. Im Fall eines **Onlineshops,**[84] der beim Softwareanbieter gehostet wird, oder bei **Backup-Dienstleistungen** ist von einer Auftragsverarbeitung auszugehen. Ebenso regelmäßig auf eine Auftragsverarbeitung gestützt wird der **Einsatz von Newsletter-Dienstleistern.**[85]

50 Entscheidend für die Beurteilung, ob eine bloße Auftragsverarbeitung vorliegt, ist stets der konkrete Einzelfall. Schon kleine Nuancen im Hinblick auf die Ausgestaltung der Dienstleistung können zu einer unterschiedlichen Bewertung führen. Praktische Bedeutung hat insofern insbesondere, dass vermeintlich kostenfreie Onlinetools sich oftmals über die Nutzung im Zusammenhang mit der Erbringung der Dienstleistung anfallender Nutzerdaten refinanzieren. Werden im Rahmen der Dienstleistung verarbeitete personenbezogene Daten auch für **eigene Zwecke** genutzt, überschreitet dies jedoch die **Grenzen der Auftragsverarbeitung.** Beispiele: Ein Onlinekartendienst, der in die Unternehmenswebsite eingebunden werden kann, benutzt die Nutzerdaten nicht nur zur Erbringung des Dienstes, sondern auch um den Dienst weiterzuentwickeln. Ein kostenfrei nutzbarer Filehosting-Dienst finanziert sich über verhaltensbasierte Onlinewerbung.

51 Praxisrelevant ist insbesondere die Frage, inwiefern das Angebot von **Webanalysetools,** mittels derer Daten über Besucherzahlen, Besuchsdauer und Besucherverhalten zum Zwecke der Optimierung des Angebotes erlangt werden können, eine Auftragsverarbeitung darstellt. Eine Ausgestaltung als Auftragsverarbeitung ist möglich, setzt allerdings, wie dargestellt, voraus, dass die erhobenen Informationen ausschließlich weisungsgebunden im Interesse des Auftraggebers verarbeitet werden. Sofern der Anbieter etwa websiteübergreifende Nutzerprofile erstellt oder Daten aus der Webanalyse mit Nutzerdaten aus anderen von ihm angebotenen Diensten zusammenführt, ist dies über eine Auftragsverarbeitung nicht mehr gedeckt.[86] Zur Frage der Zulässigkeit von personenbezogenen Datenverarbeitun-

[82] So nunmehr auch Simitis/Hornung/Spiecker gen. Döhmann/Boehm DSGVO Art. 82 Rn. 23.
[83] Kühling/Buchner/Hartung DS-GVO Art. 28 Rn. 103.
[84] Zur datenschutzrechtlichen Verantwortlichkeit im Zusammenhang mit Onlineshops oder dem Vertrieb über Online-Verkaufsplattformen vgl. auch → Kap. 23 Rn. 4 ff.
[85] Koreng/Lachenmann DatenschutzR-FormHdB/Lachenmann Form. F.I.4. Anm. 4.
[86] Forgó/Helfrich/Schneider Betr. Datenschutz-HdB/Conrad/Dovas Teil IX Kap. 2 Rn. 110.

gen und Endgerätzugriffen im Zusammenhang mit der Webanalyse vgl. im Einzelnen → Kap. 9 Rn. 88 ff.

Im Fall von Angeboten, welche auf **Cloud Computing** basieren, ergeben sich zusätzliche datenschutzrechtliche Herausforderungen, sofern nicht sichergestellt ist, dass das Cloud-Computing-Netzwerk auf den europäischen Raum beschränkt bzw. auf solche Staaten, für die ein angemessenes Datenschutzniveau festgestellt ist. Denn in diesem Fall sind die speziellen Anforderungen der DS-GVO an einen **sog. Drittlandtransfer** zu berücksichtigen. Zum Drittlandtransfer vgl. im Einzelnen → Rn. 118 und → Kap. 13 Rn. 1 ff. 52

6. Abgrenzung alleinige und gemeinsame Verantwortlichkeit

Steht fest, dass es sich bei mehreren Beteiligten einer Onlinedatenverarbeitung jeweils um Verantwortliche iSv Art. 4 Nr. 7 DS-GVO handelt, ist in einem zweiten Schritt zu ermitteln, **in welchem Verhältnis die Verantwortlichen zueinanderstehen:** Handelt es sich um jeweils eigenständig datenschutzrechtlich Verantwortliche (Art. 4 Nr. 7 Hs. 1 Alt. 1 DS-GVO) oder aber liegt ein Fall der gemeinsamen Verantwortlichkeit vor (Art. 4 Nr. 7 Hs. 1 Alt. 2 DS-GVO, Art. 26 DS-GVO)? 53

Die Zweckbestimmung von Art. 26 DS-GVO ergibt sich insbesondere aus Erwgr. 79 DS-GVO. Danach bedarf es zum **Schutz der Rechte und Freiheiten der betroffenen Personen** sowie bezüglich der Verantwortung und Haftung der Verantwortlichen – auch mit Blick auf die Überwachungs- und sonstigen Maßnahmen von Aufsichtsbehörden – einer klaren **Zuteilung der Verantwortlichkeiten aus der DS-GVO.** Betroffene Personen sollen nicht schlechter gestellt werden, sofern mehrere Akteure für die Datenverarbeitung verantwortlich sind. Primäres Ziel ist also die Wahrung von Transparenz und Betroffenenrechten auch im Rahmen der komplexen modernen Datenverarbeitungszusammenhänge. Insbesondere soll die betroffene Person wissen, wohin sie sich mit einem Berichtigungsanspruch, Löschungsbegehren etc wenden kann. 54

Wie bereits dargestellt,[87] ist die Möglichkeit einer gemeinsamen datenschutzrechtlichen Verantwortlichkeit keine Neuerung durch die DS-GVO, sondern das Prinzip war bereits in der DS-RL angelegt, die der DS-GVO vorausging. Wie ebenfalls schon ausgeführt, hat das Rechtsinstitut der gemeinsamen Verantwortlichkeit erhöhte Aufmerksamkeit jedoch erst mit den diesbezüglichen EuGH-Entscheidungen aus den Jahren 2018 und 2019[88] erfahren. Nicht von der Hand zu weisen ist allerdings, dass, obwohl die Rechtsfigur der gemeinsamen Verantwortlichkeit durch die EuGH-Rechtsprechung stärkere Konturierung erfahren hat, in der Praxis nach wie vor ein **Widerstand gegen das Rechtsinstitut** zu spüren ist. Vermutlich insbesondere angesichts der haftungsrechtlichen Implikationen bemühen sich die Verantwortlichen, Verarbeitungsverfahren mit mehreren Beteiligten nach Möglichkeit aus der gemeinsamen Verantwortlichkeit herauszuhalten und in Richtung einer getrennten datenschutzrechtlichen Verantwortlichkeit der Beteiligten oder aber in Richtung von Auftragsverarbeitungsbeziehungen zu rücken. Die Gestaltungsfreiheit ist insoweit allerdings eingeschränkt.[89] 55

Wie die Stellung als (allein) Verantwortlicher knüpft auch die Rolle der gemeinsam für die Datenverarbeitung Verantwortlichen an die Entscheidung über Mittel und Zwecke der Datenverarbeitung an. 56

[87] Vgl. iE → Rn. 5.
[88] EuGH 5.6.2018 – C-210/16, BeckRS 2018, 10155 – Facebook-Fanpages; 10.7.2018 – C-25/17, ZD 2018, 469 – Zeugen Jehovas; 29.7.2019 – C-40/17, BeckRS 2019, 15831 – Fashion ID, vgl. zu den Entsch. iE → Rn. 58 ff.
[89] Vgl. → Rn. 84 f.

57 Nach Art. 26 Abs. 1 S. 1 DS-GVO sind zwei oder mehr Verantwortliche iSv Art. 4 Nr. 7 DS-GVO, sofern sie **Zwecke und Mittel der Verarbeitung gemeinsam festlegen,** gemeinsam verantwortlich im Sinne des Datenschutzrechts. Maßgeblich ist insofern ein „funktioneller Ansatz und eine Betrachtung der tatsächlichen Beziehungen".[90]

58 Der **EuGH** hat sich zunächst 2018 und 2019 in drei grundlegenden Entscheidungen zur gemeinsamen Verantwortlichkeit geäußert und dabei überraschend **geringe Anforderungen** an eine solche gemeinsame Entscheidung gestellt:
- EuGH 5.6.2018 – C-210/16 – Facebook-Fanpages
- EuGH 10.7.2018 – C-25/17 – Zeugen Jehovas
- EuGH 29.7.2019 – C-40/17 – Fashion ID

59 Die Interpretation der europäischen Aufsichtsbehörden zu Art. 26 DS-GVO ergibt sich maßgeblich aus den vom **EDSA** erlassenen **Leitlinien 7/2020** zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DS-GVO. Die Version 2.0 dieses Dokuments wurde am 7.7.2021 angenommen und erging unter Berücksichtigung der aufgezählten EuGH-Entscheidungen. Das **Kurzpapier Nr. 16 der nationalen DSK** zur gemeinsamen Verantwortlichkeit datiert noch aus 2018 und befindet sich in Überarbeitung. Die geplante Neufassung des DSK-Papiers soll insbesondere die Version 2.0 der EDSA-Leitlinie berücksichtigen.

60 Die erste der drei grundlegenden EuGH-Entscheidungen zur gemeinsamen Verantwortlichkeit betraf die Frage, inwiefern der Betreiber einer **Facebook-Fanpage** gemeinsam mit Facebook für die Verarbeitung der personenbezogenen Daten der Besucher der Fanpage verantwortlich ist.[91] Insofern stellte der EuGH fest, dass allein der Umstand der Nutzung eines sozialen Netzwerks wie Facebook für sich betrachtet den Nutzer, also diejenige Stelle, welche die Fanpage betreibt, nicht für die von der Plattform durchgeführte Datenverarbeitung mitverantwortlich macht.[92]

61 Eine gemeinsame Verantwortlichkeit hat der EuGH aber im Hinblick auf die konkret beklagte Wirtschaftsakademie Schleswig-Holstein angenommen, soweit die Verarbeitung der personenbezogenen Daten der Besucher von deren Fanpage durch Facebook betroffen war. Im Hinblick auf die Umstände im konkreten Fall sei festzustellen, so der EuGH, dass „der Betreiber einer auf Facebook unterhaltenen Fanpage […] durch die von ihm vorgenommene Parametrierung u.a. entsprechend seinem Zielpublikum sowie den Zielen der Steuerung oder Förderung seiner Tätigkeiten an der Entscheidung über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten der Besucher seiner Fanpage beteiligt ist".[93] Die Möglichkeit, auf den Endgeräten der Fanpagebesucher Cookies zu setzen und in der Folge statistische Auswertungen über deren Verhalten zu erstellen, werde durch Schaltung der Fanpage erst eröffnet, so der EuGH.[94] Der Betreiber der Fanpage trage insofern zur Verarbeitung der personenbezogenen Daten der Seitenbesucher bei[95] und könne insbesondere von Facebook demografische Daten über seine Zielgruppe verlangen sowie geografische Daten, welche es ihm ermöglichten, sein Informationsangebot möglichst zielgerichtet auszugestalten.[96]

62 Auch wenn der Fanpagebetreiber die Besucherstatistiken ausschließlich in anonymisierter Form übermittelt bekomme, so basiere doch die Erstellung der Statistiken auf der vorhergehenden Erhebung personenbezogener Daten der Fanpagebesucher – mittels der von Facebook gesetzten Cookies – und der anschließenden Verarbeitung dieser Daten für sta-

[90] Kühling/Buchner/Hartung DS-GVO Art. 26 Rn. 13 mwN.
[91] EuGH 5.6.2018 – C-210/16, BeckRS 2018, 10155 – Facebook-Fanpages.
[92] EuGH 5.6.2018 – C-210/16, BeckRS 2018, 10155 Rn. 35 – Facebook-Fanpages.
[93] EuGH 5.6.2018 – C-210/16, BeckRS 2018, 10155 Rn. 39 – Facebook-Fanpages.
[94] EuGH 5.6.2018 – C-210/16, BeckRS 2018, 10155 Rn. 35 – Facebook-Fanpages.
[95] EuGH 5.6.2018 – C-210/16, BeckRS 2018, 10155 Rn. 36 – Facebook-Fanpages.
[96] EuGH 5.6.2018 – C-210/16, BeckRS 2018, 10155 Rn. 37 – Facebook-Fanpages.

tistische Zwecke.[97] Eine gemeinsame Verantwortlichkeit setze **keine gleichwertige Verantwortung** voraus, so der EuGH in der Fanpageentscheidung, oder auch nur, dass jeder beteiligte Verantwortliche **Zugang** zu den betreffenden personenbezogenen Daten habe.[98]

63 Im Nachgang zur Fanpage-Entscheidung des EuGH entschied das vorlegende nationale BVerwG, dass der Betreiber eines solchen Social-Media-Auftritts verpflichtet werden kann, die Fanpage abzuschalten, sofern die von Facebook zur Verfügung gestellte digitale Infrastruktur schwerwiegende datenschutzrechtliche Mängel aufweist.[99] Zur Frage der Rechtswidrigkeit der im Einzelnen beanstandeten Datenverarbeitungsvorgänge verwies das BVerwG die Sache an die Vorinstanz zurück, das OVG Schleswig. Letzteres entschied sodann, dass die Wirtschaftsakademie Schleswig-Holstein als Beklagte des Ausgangsverfahrens ihre Facebook-Fanpage abschalten muss.[100]

64 Den Aspekt, dass eine gleichwertige Verantwortlichkeit nicht notwendig ist und nicht jeder Verantwortliche Zugang zu den personenbezogenen Daten haben muss, hat der EuGH auch in seiner nachfolgenden Entscheidung zur Verkündigungstätigkeit der **Zeugen Jehovas** an Haustüren nochmals betont.[101] In dieser Entscheidung urteilte der EuGH, dass eine Religionsgemeinschaft wie die der Zeugen Jehovas gemeinsam mit ihren als Verkündiger tätigen Mitgliedern für die Verarbeitung der personenbezogenen Daten verantwortlich ist, die im Rahmen einer von Tür zu Tür durchgeführten Verkündigungstätigkeit erhoben werden. Dadurch, dass sie die Verkündigungstätigkeit „organisiert und koordiniert und zu ihr ermuntert" hat, habe die Religionsgemeinschaft gemeinsam mit den verkündigenden Mitgliedern an der Entscheidung über die Zwecke und Mittel der Datenverarbeitung mitgewirkt, so der EuGH in der Entscheidung.[102] Eine entsprechende Mitwirkung setze nicht voraus, dass die Religionsgemeinschaft selbst Zugriff auf die betreffenden Daten oder ihren Mitgliedern Anleitungen oder Anweisungen zu den Datenverarbeitungen gegeben hat.[103] Ohne elektronische Datenverarbeitung wird in der „Zeugen Jehovas"-Konstellation nach Auffassung des EuGH eine Situation geschaffen, die mit der Sammlung personenbezogener Daten über Cookies und deren anschließender Auswertung zumindest im Ausgangspunkt – wenn auch nicht im Hinblick auf das Ausmaß der Datenverarbeitung – vergleichbar ist.

65 Im Rahmen der Rechtssache **„Fashion ID"** hatte sich der EuGH sodann mit der Beurteilung der datenschutzrechtlichen Verantwortlichkeit zu befassen, wenn Unternehmen sog. **Social Plug-ins** auf der Unternehmenswebsite einbinden.[104] Konkret ging es um den „Gefällt mir"-Button von Facebook, die Entscheidung ist aber auf andere Social Plug-ins übertragbar. Durch Einbettung entsprechender Plug-ins wird der Browser der Websitenutzer veranlasst, Inhalte des Anbieters des Plug-ins anzufordern und in diesem Zusammenhang Nutzerdaten an den Anbieter zu übermitteln. Die Einbindung des „Gefällt mir"-Buttons von Facebook durch die Fashion ID in deren Website ermögliche es dieser, „die Werbung für ihre Produkte zu optimieren, indem diese im sozialen Netzwerk Facebook sichtbarer gemacht werden", so der EuGH.[105] Zum Zweck der Erlangung wirtschaftlicher Vorteile willige Fashion ID insofern durch Integration des Buttons in die eigene Website zumindest stillschweigend in die Erhebung der Daten der Websitebesucher sowie die Weitergabe der Informationen an Facebook ein.[106] Die Verarbeitungsvorgänge würden dabei im wirtschaftlichen Interesse sowohl von Fashion ID als auch von Facebook Ireland durch-

[97] EuGH 5.6.2018 – C-210/16, BeckRS 2018, 10155 Rn. 38 – Facebook-Fanpages.
[98] EuGH 5.6.2018 – C-210/16, BeckRS 2018, 10155 Rn. 43, 38 – Facebook-Fanpages.
[99] BVerwG 11.9.2019 – 6 C 15.18.
[100] OVG Schleswig 25.11.2021 – 4 LB 20/13.
[101] EuGH 10.7.2018 – C-25/17, ZD 2018, 469 Rn. 66, 69 – Zeugen Jehovas.
[102] EuGH 10.7.2018 – C-25/17, ZD 2018, 469 Rn. 73 – Zeugen Jehovas.
[103] EuGH 10.7.2018 – C-25/17, ZD 2018, 469 Rn. 75 – Zeugen Jehovas.
[104] EuGH 29.7.2019 – C-40/17, BeckRS 2019, 15831 – Fashion ID.
[105] EuGH 29.7.2019 – C-40/17, BeckRS 2019, 15831 Rn. 80 – Fashion ID.
[106] EuGH 29.7.2019 – C-40/17, BeckRS 2019, 15831 Rn. 80 – Fashion ID.

geführt, so der EuGH.[107] Entsprechend sei davon auszugehen, dass Fashion ID und Facebook Ireland gemeinsam über die Zwecke der Datenerhebung und -weitergabe entscheiden.[108] Letztlich genügt dem EuGH damit bereits ein rein wirtschaftliches Interesse an der Datenverarbeitung als gemeinsamer Zweck. Die Einbindung des Social Media Plug-ins begründe eine gemeinsame datenschutzrechtliche Verantwortlichkeit bzgl. der Datenerhebung und -weitergabe, die über das Plug-in ausgelöst wird, so das Gericht. Sowohl der Websitebetreiber als auch der Social Media Anbieter müssten daher über eine **Rechtsgrundlage für** die entsprechenden **Verarbeitungsvorgänge** verfügen.[109]

66 Der EuGH betonte in der Rechtssache „Fashion ID" außerdem, dass eine Website wie die von Fashion ID auch von Personen besucht wird, die **keine Facebook Mitglieder** sind. Insofern erscheine die Verantwortlichkeit des Websitebetreibers, der das Plug-in einsetzt, noch höher.[110] Denn durch den bloßen Aufruf der Website durch die betroffenen Nichtmitglieder werde automatisch die Verarbeitung ihrer Daten durch Facebook ausgelöst.[111]

67 Letzteres gilt jedenfalls, wenn Social Media Plug-ins wie der Facebook „Gefällt mir"-Button in ihrer nativen Form und nicht über eine **Zwei-Klick-Lösung oder Shariff** eingebunden werden.[112]

68 Die dargestellte extensive Auslegung der gemeinsamen Verantwortlichkeit durch den EuGH dient dem nachvollziehbaren Zweck, einen möglichst umfassenden und wirksamen Schutz betroffener Personen zu ermöglichen. Die weite Auslegung des Rechtsinstituts durch den EuGH hat allerdings zugleich, wie sogar der EDSB bestätigt,[113] zu einer nicht unerheblichen **Rechtsunsicherheit** bei Stellen geführt, die an arbeitsteiligen Datenverarbeitungen beteiligt sind.[114] In der Literatur wird zum Teil auch die Vereinbarkeit der EuGH-Rechtsprechung mit den Wortlautgrenzen der DS-GVO in Zweifel gezogen.[115]

69 Abschließend können aus den dargestellten drei zentralen EuGH-Entscheidungen zur gemeinsamen Verantwortlichkeit folgende Gesichtspunkte zusammengefasst werden:

- Die Begründung einer gemeinsamen Verantwortlichkeit setzt eine gemeinsame Entscheidung über die Zwecke und (wesentlichen) Mittel der Verarbeitung voraus. Nach der EuGH-Rechtsprechung genügt es nicht, dass die gemeinsame Entscheidung nur auf einen der beiden Aspekte bezogen ist.[116] Insofern genügt es weder, wenn nur eine gemeinsame Infrastruktur verwendet wird ohne dass verbundene Zwecke bestehen, noch, dass zwar ein gemeinsamer Zweck besteht, aber unterschiedliche Mittel eingesetzt werden.[117]
- Gemeinsame Verantwortlichkeit erfordert nicht, dass jeder beteiligte Akteur hinsichtlich der Verarbeitung **identische Handlungsoptionen** hat. Gemeinsame Verantwortlichkeit ist also nicht im Sinne einer gleichwertigen Verantwortlichkeit zu verstehen und erfor-

[107] EuGH 29.7.2019 – C-40/17, BeckRS 2019, 15831 Rn. 80 – Fashion ID.
[108] EuGH 29.7.2019 – C-40/17, BeckRS 2019, 15831 Rn. 81 – Fashion ID.
[109] EuGH 29.7.2019 – C-40/17, BeckRS 2019, 15831 Rn. 97 – Fashion ID.
[110] EuGH 29.7.2019 – C-40/17, BeckRS 2019, 15831 Rn. 83 – Fashion ID.
[111] EuGH 29.7.2019 – C-40/17, BeckRS 2019, 15831 Rn. 83 – Fashion ID. Für Nutzer aus Europa hat Facebook insofern allerdings inzwischen das Verfahren angepasst. Für Nutzer aus Europa werden die sozialen Plug-ins „Gefällt mir" und „Kommentieren" nur noch unterstützt, wenn die Nutzer bei ihrem Facebook-Konto angemeldet sind und ihre Zustimmung zu Cookies für Apps und Websites erteilt haben, vgl. developers.facebook.com/docs/plugins/like-button/?locale=de_DE.
[112] Vgl. hierzu iE → Rn. 111 ff.
[113] EDSB, Leitlinien des EDSB zu den Begriffen „Verantwortlicher", „Auftragsverarbeiter" und „gemeinsam Verantwortliche" nach der Verordnung (EU) 2018/1725, 7.11.2019, 26.
[114] Schwartmann/Jaspers/Thüsing/Kugelmann/Kremer DS-GVO Art. 26 Rn. 63.
[115] Schwartmann/Jaspers/Thüsing/Kugelmann/Kremer DS-GVO Art. 26 Rn. 62.
[116] Schwartmann/Jaspers/Thüsing/Kugelmann/Kremer DS-GVO Art. 26 Rn. 61.
[117] Schwartmann/Jaspers/Thüsing/Kugelmann/Kremer DS-GVO Art. 26 Rn. 61.