datenschutz-berater.de

44. Jahrgang DSB 11/2020

DATENSCHUTZ-BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

ISSN 0170-7256

dfv Mediengruppe

Tilman Herbrich

EDSA: Neue Leitlinien zum Konzept der Verantwortlichkeit und Auftragsverarbeitung in der DSGVO

Der Europäische Datenschutzausschuss (EDSA) veröffentlichte im September 2020 einen Entwurf für neue Leitlinien zum Konzept der Verantwortlichkeit und Auftragsverarbeitung in der DSGVO. Das Echo auf die „Guidelines 07/2020 on the concepts of controller und processor in the GDPR" ist groß. Mehr als 100 Verbände, Organisationen, Unternehmen und öffentliche Stellen haben im Rahmen der öffentlichen Konsultation ihr Feedback bis zum Teilnahmeschluss am 19. Oktober 2020 eingereicht.

Datenschutzrechtliche Verantwortlichkeit

Das Konzept des EDSA für die Festlegung von für die Verarbeitung Verantwortlichen, gemeinsamen Verantwortlichen und Auftragsverarbeitern knüpft an die Kriterien der Artikel 29-Datenschutzgruppe an, die der mehr als zehn Jahre zurückliegenden „Stellungnahme 1/2010 zu den Begriffen für die Verarbeitung Verantwortlicher und Auftragsverarbeiter" zugrunde liegen. Die Aktualisierung der Leitlinien ist insbesondere mit Blick auf Abgrenzungsfragen bei der Rollenverteilung zwischen mehreren Beteiligten begrüßenswert. Denn die Festlegung, Verteilung und Zurechnung der datenschutzrechtlichen Verantwortlichkeit ist zentraler Ausgangspunkt für die Bestimmung des datenschutzrechtlichen Pflichtenprogramms, der Umsetzung von Betroffenenrechten und Handhabung von Haftungsfragen. Aus gutem Grund verlangt deshalb Erwägungsgrund 79 DSGVO zum Schutz der Rechte und Freiheiten betroffener Personen sowie der Verantwortlichkeit und Haftung der (gemeinsam) Verantwortlichen und Auftragsverarbeiter eine klare Zuteilung der Verantwortlichkeiten.

Definition „Verantwortlicher"

Ausgehend von der Legaldefinition des für die Verarbeitung Verantwortlichen gemäß Art. 4 Nr. 7 DSGVO greifen die Leitlinien des EDSA die einzelnen Tatbestandsmerkmale auf (Rn. 15 ff.). Besonderes Augenmerk legt der EDSA dabei auf das Merkmal „Entscheidungsbefugnis". Das Datenschutzgremium hält am funktionalen Konzept zur Verantwortlichkeitsbestimmung fest, welches ursprünglich in der Stellungnahme der Artikel 29-Datenschutzgruppe entwickelt wurde. Die Festlegung der Verantwortlichkeit könne demnach zum einen aus gesetzlichen Regelungen (z. B. § 67 Abs. 4 SGB X, § 11 Abs. 2 StBerG) und zum anderen aus der tatsächlichen Einflussnahme auf die Verarbeitung unter Berücksichtigung aller relevanten faktischen Umstände folgen (Rn. 23 ff.). Das funktionale Verständnis befindet sich auf einer Linie mit der weiten Auslegung des Verantwortlichkeitsbegriffs durch den EuGH, um aus der Perspektive des Betroffenen einen effektiven Grundrechtsschutz (Art. 7 und Art. 8 GRC) zu gewährleisten.

Definition „gemeinsam Verantwortliche"

Auch für die Einordnung von gemeinsam Verantwortlichen soll ein funktionales Verständnis gelten (Rn. 49 f.). Vertragliche Regelungen könnten danach auch als Indiz für die Verantwortlichkeitsfestlegung herangezogen werden, müssten jedoch die tatsächlichen Gegebenheiten in der Realität wiederspiegeln.

Zur Bestimmung der gemeinsamen Festlegung der Zwecke und Mittel als maßgebliches Kriterium für die Qualifikation gemeinsam Verantwortlicher nach Art. 26 Abs. 1 Satz 1 DSGVO greift der EDSA auf die vom EuGH in den Rechtssachen „Wirtschaftsakademie" (EuGH, Urt. v. 5.6.2018 – C-210/16), „Zeugen Jehovas" (EuGH, Urt. v. 10.7.2018 – C-25/17) und „Fashion ID" (EuGH, Urt. v. 29.7.2019 – C-40/17) entwickelten Grundsätze zurück (Rn. 53 ff.). Entsprechend rezipiert der EDSA, dass es weder einer gleichwertigen Verarbeitung bedürfe noch ein Zugang zu den Dateninstanzen erforderlich sei. Ebenso sei keine Anleitung oder Anweisung in Bezug auf die Verarbeitung notwendig. In der Folge erkennt der EDSA auch die vom EuGH präferierte phasenspezifische Verantwortlichkeit an, wonach sich die gemeinsame Verantwortlichkeit nicht mehr auf nachgelagerte Verarbeitungsprozesse erstreckt, in denen ein Verantwortlicher allein die Zwecke und Mittel der Verarbeitung festlegt. Deshalb kann das Rollenverständnis von Beteiligten laut EDSA je nach Verarbeitungsvorgang i. S. d. Art. 4 Nr. 2 DSGVO unterschiedlich qualifiziert werden.

In Bezug auf die gemeinsame Festlegung der Zwecke der Verarbeitung betont der EDSA, dass keine Zweckidentität erforderlich sei, vielmehr reiche eine Verbundenheit und Ergänzung der Zwecke aus (Rn. 58 ff.). Demgegenüber soll ein bloßer Vorteil aus der Verarbeitung noch keine gemeinsame Zweckfestlegung begründen. Entsprechend der EuGH Rechtsprechung nimmt der EDSA eine gemeinsame Entscheidung über die Mittel der Verarbeitung bei der Nutzung fremder Plattformen, standardisierter Tools (z. B. Tracking-Codes) oder anderer Infrastrukturen an, die ein Beteiligter einem anderen für die Verarbeitung zu gemeinsamen Zwecken zur Verfügung stellt.

Hilfreich für der Praxis dürfte die Einschränkung des EDSA sein, dass selbst in den zuvor benannten Fällen eine gemeinsame Verantwortlichkeit ausscheide, wenn die Verarbeitung trennbar und ohne Intervention des anderen Beteiligten durchführbar sei oder es an einer gemeinsamen Zweckbestimmung fehle. Spezifische Fallgruppen für die Verantwortlichkeitsverteilung im Kontext sozialer Netzwerke finden sich in den lesenswerten Leitlinien 08/2020 des EDSA zum Targeting von Nutzern sozialer Netzwerke (vgl. hierzu Siebelmann, DSB 2020, 246).

Beispielhaft bejaht der EDSA eine gemeinsame Verantwortlichkeit von Online-Buchungsplattformen und Fluggesellschaften bzw. Hotels bei gemeinsamen Marketingaktionen auf Grundlage gemeinsam gesammelter Kundendaten, von Unternehmen bei der Vermarktung von Co-Branding-Produkten auf gemeinsamen Veranstaltungen oder Werbemitteln, von Kliniken und Sponsoren bei der Durchführung klinischer Tests sowie von Headhuntern und Arbeitgebern bei Recruiting-Prozessen. Der EDSA spricht sich andererseits gegen die Annahme einer gemeinsamen Verantwortlichkeit aus bei eigenständigen Werbeaktionen von Unternehmen einer Unternehmensgruppe trotz Nutzung einer gemeinsamen Datenbasis, bei Hosting-Tätigkeiten oder bei Übermittlungen von Daten an Steuerbehörden.

Definition „Auftragsverarbeiter"

Auch bei der Klassifizierung von Auftragsverarbeitern hält der EDSA an den Ausführungen der Artikel 29-Datenschutzgruppe fest. Ausgehend von Art. 4 Nr. 8 DSGVO stellt der EDSA die Auftragsverarbeitung unter zwei Voraussetzungen: Es muss sich bei dem Auftragsverarbeiter um eine unabhängige Stelle handeln und die Verarbeitung muss im Auftrag des Verantwortlichen erfolgen. Während Zwecke stets nur vom Verantwortlichen im Auftrag festgelegt werden dürften, erachtet der EDSA eine Delegation nicht wesentlicher Mittel der Verarbeitung als zulässig an und räumt den Auftragsverarbeitern insofern wie bislang einen Ermessensspielraum ein (Rn. 78). Zu den wesentlichen Mitteln der Verarbeitung, deren Entscheidung ausschließlich dem Verantwortlichen vorbehalten ist, zählt der EDSA die Festlegung der Art der Daten, Kategorien betroffener Personen, Speicherdauer und Zugangsmöglichkeiten. Hingegen könnten nicht wesentliche Mittel, insbesondere die Auswahl von Hard- und Software oder spezifische Maßnahmen der Datensicherheit, auf den Auftragsverarbeiter delegiert werden (Rn. 38).

Die für die Praxis entscheidende Frage, ob Auftragsverarbeiter – z. B. bei Beauftragung einer Marketingagentur zur Erstellung von Werbemitteln – Daten auch zur Verbesserung der eigenen Produkte und Dienstleistungen verwendet werden dürfen, beantwortet der EDSA anhand von Art. 28 Abs. 10 DSGVO. Ein Auftragsverarbeiter, der unter Verstoß gegen die Pflichten der DSGVO eigene Zwecke und Mittel der Verarbeitung weisungswidrig bestimmt und sich zum eigenständigen Verantwortlichen aufschwingt, kann nach Ansicht des EDSA Adressat von Sanktionen der Aufsichtsbehörden werden.

Grundsätzlich grenzt der EDSA die Auftragsverarbeitung zur eigenständigen Verantwortlichkeit von Dritten i. S. d. Art. 4 Nr. 10 DSGVO ab (Rn. 86 f.). Leider äußert sich das Gremium lediglich punktuell zur generellen Behandlung von konzernweiten Verarbeitungen und verneint jedenfalls eine Auftragsverarbeitung, wenn eine Muttergesellschaft z. B. Beschäftigtendaten der einzelnen Unternehmen der Gruppe zu Analysezwecken verarbeitet (Rn. 87).

Im Allgemeinen spricht sich der EDSA für eine „case-by-case" Analyse insbesondere in Bezug auf die Nutzung von Cloud-Anbietern für Onlinespeicher- oder Messenger-Dienste sowie Videokonferenzen aus, um den Grad der Einflussnahme auf die Zwecke und Mittel der Verarbeitung im Einzelfall zu bestimmen (Rn. 80 ff.). Auch die Beauftragung von Callcenter-Dienstleistungen und generellem IT-Support sollen regelmäßig der Auftragsverarbeitung unterfallen. Zutreffend lehnt der EDSA eine Auftragsverarbeitung bei der Inanspruchnahme von bloßen Taxi-Bestellungen, Reinigungsdiensten und IT-Wartungsarbeiten ab.

Verhältnis zwischen Beteiligten einer Verarbeitung

Im zweiten Teil der Leitlinien werden die datenschutzrechtlichen Pflichten (Rn. 91 ff.) für das jeweilige Verhältnis zwischen den Beteiligten herausgestellt.

Verhältnis zu Auftragsverarbeitern

Kennzeichnend für die Auftragsverarbeitung ist die volle Verantwortlichkeit des Auftraggebers für die Datenverarbeitung durch einen Auftragsverarbeiter, wenngleich bestimmte Pflichten (z. B. für Datensicherheit oder Drittstaatentransfer) auch an Auftragsverarbeiter adressiert werden.

Der EDSA stellt hohe Anforderungen an die Auswahlverantwortlichkeit von Auftragsverarbeitern gemäß Art. 28 Abs. 1 DSGVO und geht dabei von einer fortlaufenden Prüfpflicht für die in Erwägungsgrund 81 DSGVO genannten Kriterien (Fachwissen, Zuverlässigkeit und Ressourcen) aus (Rn. 92 ff.). Hierfür sei ein „Risk Assessment" in Bezug auf den Auftragsverarbeiter durchzuführen. Hinreichende Garantien für den Einsatz technischer und organisatorischer Maßnahmen (Art. 32 DSGVO), welche die Einhaltung der Pflichten aus der DSGVO und die Sicherstellung der Betroffenenrechte gewährleisten, sollen sich dabei aus vorhandenen Dokumentationen des Auftragsverarbeiters ergeben. Dazu zählen laut EDSA Datenschutzhinweise, Nutzungsbedingungen, Verfahrensverzeichnisse, IT-Sicherheitsrichtlinien sowie internationale Zertifizierungen wie z. B. die ISO 27000-Serien. Daneben kommen

freilich gemäß Art. 28 Abs. 5 DSGVO genehmigte Verhaltensregeln (Art. 40 DSGVO) und genehmigte Zertifizierungsverfahren (Art. 42 DSGVO) in Betracht.

Die Verpflichtung zum Abschluss eines Auftragsverarbeitungsvertrages nach Maßgabe von Art. 28 Abs. 3 DSGVO trifft nach Ansicht des EDSA sowohl den Verantwortlichen als auch den Auftragsverarbeiter. Dabei akzeptiert der EDSA explizit die in der Praxis anzutreffende Ausgestaltung innerhalb von AGB. Bezogen auf den Inhalt des Vertrages nach Art. 28 Abs. 3 DSGVO lässt der EDSA (Rn. 108 ff.) eine bloße Wiedergabe des Gesetzeswortlautes nicht ausreichen und fordert eine dem Risiko für Betroffene angemessene Konkretisierung der vertraglichen Inhalte und Verpflichtungen zur Ergreifung bestimmter Maßnahmen. Dabei bieten die Leitlinien des EDSA wertvolle Hinweise für eine datenschutzkonforme Ausgestaltung. So erachtet der EDSA Weisungen des Verantwortlichen in Bezug auf jeden Verarbeitungsvorgang für notwendig und empfiehlt eine detaillierte Auflistung im Anhang des Vertrags. Sofern eine Datenverarbeitung in einem Drittstaat geplant ist, soll der Vertrag über die Auftragsverarbeitung die Anforderungen nach Art. 44 ff. DSGVO unter Berücksichtigung der „Schrems II"-Entscheidung des EuGH (EuGH, Urt. v. 16.7.2020 – C-311/18) aufführen. Auf die Zulässigkeit von Klauseln zur Haftungsfreistellung geht der EDSA leider nicht ein.

Folgen einer gemeinsamen Verantwortlichkeit

Im Gegensatz zur Auftragsverarbeitung gesteht der EDSA bei der Ausgestaltung der Vereinbarung nach Art. 26 Abs. 1 Satz 2 DSGVO den Parteien wesentlich flexiblere Gestaltungsmöglichkeiten ein (Rn. 158 ff.). Über die gesetzlichen Mindestinhalte hinaus – Wahrnehmung Betroffenenrechte und Erfüllung Informationspflichten – sei in jedem Fall die Festlegung der gemeinsamen Verarbeitungsvorgänge, Zwecke sowie Kategorien personenbezogenen Daten und betroffener Personen notwendig. Nützlich erweist sich die Empfehlung der Leitlinien, zu konkretisieren, welche Partei für folgende Aspekte der Verarbeitung verantwortlich ist: Bereitstellung von Datenschutzhinweisen, Beantwortung von Betroffenenanfragen, Sicherstellung der Datenschutzgrundsätze, Nachweis einer Rechtsgrundlage, Umsetzung technischer und organisatorischer Maßnahmen, Meldungen im Fall von Datenschutzvorfällen, Durchführung von Datenschutz-Folgeabschätzungen, Einschaltung von Auftragsverarbeitern, Drittstaatentransfer, Anlaufstelle für Betroffenenanfragen und Aufsichtsbehörden. Für die Praxis besonders in Haftungsfällen relevant ist, dass der EDSA Haftungsklauseln für den Fall der Nichteinhaltung der fixierten vertraglichen Pflichten akzeptiert (Rn. 171).

Hilfreich sind vor allem die Ausführungen zum Umgang mit den besonderen Informationspflichten aus Art. 26 Abs. 2 Satz 2 DSGVO (Rn. 178 f.). Zum einen solle das „Wesentliche der Vereinbarung" zumindest die Elemente enthalten, die sich im Katalog für die allgemeinen Datenschutzhinweise nach Art. 13 und Art. 14 DSGVO wiederfinden. Zum anderen könnten diese Informationen in die allgemeinen Datenschutzhinweise nach Art. 13 und Art. 14 DSGVO aufgenommen werden. Damit ermöglicht der EDSA einen praxistauglichen Umgang und überspannt zugleich nicht den Umfang der Informationspflichten.

Fazit und Hinweise für die Praxis

In der Praxis ist nach rund zweieinhalb Jahren seit Geltung der DSGVO ein sog. Repapering-Verfahren zu empfehlen, d. h. eine Überarbeitung der datenschutzrechtlichen Vertragsstrukturen. Dabei ist sorgfältig anhand einer einzelfallbezogenen Analyse zu prüfen, ob eine Auftragsverarbeitung, eine getrennte oder gemeinsame Verantwortlichkeit vorliegt. Man ist gut beraten, sich im Grundsatz an den Leitlinien des EDSA zu orientieren. Denn den Leitlinien des EDSA kommt ein hohes Gewicht vor allem bei Überprüfungen durch nationale Aufsichtsbehörden zu.

Die Ausdifferenzierung von Detailfragen vermag das Papier des EDSA nicht leisten zu können. Angesprochen sind z. B. Verarbeitungen für ein „Fraud Risk Scoring", d. h. beim Abgleich von Kundendaten des Verantwortlichen mit einer eigenen Datenbank eines Auftragsverarbeiters und Übermittlung von Scorewerten ohne Nutzung der Daten zu eigenen Zwecken. Die Klärung solcher Grenzfälle wird nicht zuletzt Aufgabe künftiger Rechtsprechung sein. Die Checkliste im Anhang der Leitlinien des EDSA bietet einen praxistauglichen Ausganspunkt für die Beurteilung der Zusammenarbeit mit anderen Akteuren und Evaluierung des eigenen Vertragsmanagements. Im Rahmen eines Stufenmodells lässt sich die Checkliste auf die Bedürfnisse des Verantwortlichen und Auftragsverarbeiters anpassen und weiterentwickeln. Sämtlich Beteiligten ist zu empfehlen, interne Analysen zur Festlegung von Rollen sowie das Bemühen um einen zutreffenden Vertragsschluss im ausreichenden Maße zu dokumentieren, um den Nachweis- und Rechenschaftspflichten aus Art. 5 Abs. 2 und Art. 24 Abs. 1 DSGVO nachzukommen. Dies gilt erst recht, wenn aufgrund von Machtdisparitäten zwischen Verhandlungspartnern eine Einflussnahme auf die Festlegung des Vertragstypus faktisch ausgeschlossen ist. Auf diesem Wege lässt sich einer etwaigen aufsichtsbehördlichen Sanktionierung aufgrund einer unzutreffenden vertraglichen Einordnung präventiv entgegenwirken und gegebenenfalls reduzieren.

Autor: **Tilman Herbrich (CIPP/E) ist Teil der Schriftleitung und Rechtsanwalt bei Spirit Legal LLP in Leipzig. Als Privacy Expert berät er Unternehmen bei der Nutzung neuer Werbetechnologien im Einklang mit dem Europäischen Datenschutz- und Wettbewerbsrecht.**