Kommunikation & Recht

K&R

2 | Februar 2024
27. Jahrgang
Seiten 85 - 156

www.kommunikationundrecht.de

dfv Mediengruppe
Frankfurt am Main

Sowohl die Ausführungen zur Einbeziehung der Datenschutzhinweise in die AGB-Kontrolle von vorformulierten Einwilligungen als auch die Überlegungen zu den rechtlichen Anforderungen an zulässige Drittlandtransfers sind nachvollziehbar begründet. Der Schutz der Verbraucher bzw. der betroffenen Personen steht hier im Vordergrund, was jedoch nicht bedeutet, dass die materiell-rechtlichen Anforderungen an die datenverarbeitenden Unternehmen dadurch erhöht wurden. Diese sollten vielmehr der Gestaltung ihrer Datenschutzhinweise und Cookie-Banner besondere Beachtung schenken, um Risiken aufgrund von unpräzisen Verweisen, unnötigen Verlinkungen und/oder nachlässigen Formulierungen zu vermeiden.

Susanne Klein
Partnerin bei ADVANT Beiten in Frankfurt a. M., Fachanwältin für IT-Recht und externe Datenschutzbeauftragte (TÜV Nord zert.); Spezialisierung auf Datenschutzrecht insbesondere in den Bereichen digitale Medien, Technologie und Healthcare; Mitglied der Deutschen Gesellschaft für Recht und Informatik (DGRI), davit und des EULISP-Alumni Deutschland e. V.

RA Dr. Patrick Grosmann und RA Dr. Hauke Hansen*

Neues zur Haftung von Auftragsverarbeitern und Verantwortlichen

Zugleich Kommentar zu EuGH, Urteil vom 5. 12. 2023 – C-683/21, K&R 2024, 119 ff. (in diesem Heft)

Kurz und Knapp

Die Verhängung einer Geldbuße gegen den Verantwortlichen setzt stets einen Verschuldensnachweis voraus. Der Verantwortliche haftet auch für DSGVO-Verstöße des Auftragsverarbeiters, es sei denn, dass der Auftragsverarbeiter Daten zu eigenen Zwecken verarbeitet oder die vertraglichen Grenzen des Auftragsverarbeitungsvertrags überschritten werden. Der Abschluss eines Joint-Controllership-Vertrags ist kein konstitutives Merkmal für das Bestehen einer Verarbeitung in gemeinsamer Verantwortlichkeit.

I. Einleitung

Der EuGH hat einen weiteren Beitrag zu der praxisrelevanten Abgrenzung der datenschutzrechtlichen Verantwortlichkeiten (Auftragsverarbeitung, gemeinsame Verantwortlichkeit und Verarbeitung in eigener Verantwortlichkeit (Controller to Controller)) geleistet. Auf die Vorlage eines litauischen Verwaltungsgerichts, das über eine Geldbuße aufgrund einer unrechtmäßigen Datenverarbeitung im Zusammenhang einer Covid-App zu entscheiden hatte, hat der EuGH unter anderem zur datenschutzrechtlichen Verantwortlichkeit entschieden.

II. Das Ausgangsverfahren

Dem Ausgangsverfahren lag eine Geldbuße gegen das NZÖG – eine Behörde des Gesundheitsministeriums – und gegen ITSS – ein beauftragtes IT-Unternehmen zur Entwicklung einer Covid-App – zugrunde. Dem NZÖG wurde ein Verstoß gegen die Artt. 5, 13, 24, 32 und 35 DSGVO vorgeworfen und das ITSS zugleich als gemeinsamer Verantwortlicher in Anspruch genommen. Die App wurde für ca. 1,5 Monate zum Download bereitgestellt und von 3802 Menschen genutzt. Neben Daten zur Person und zum Aufenthaltsort wurden in der App auch Daten zum Gesundheitszustand erhoben. Vertragliche Vereinbarungen zum Erwerb der App durch das NZÖG wurden zwischen dem NZÖG und dem ITSS nicht getroffen.

In dem Ausgangsverfahren streitet das NZÖG für eine alleinige datenschutzrechtliche Verantwortlichkeit des ITSS. Das ITSS geht dagegen von einer Verarbeitung der Daten im Auftrag des NZÖG aus.

III. Die Entscheidung des EuGH

Das Gericht hat eine wichtige Entscheidung zur Haftung des Verantwortlichen für dessen Auftragsverarbeiter gefällt.

1. Verantwortlichkeit bei einer Beauftragung zur App-Entwicklung

In den ersten drei Vorlagefragen hatte der EuGH darüber zu entscheiden, ob eine Stelle, die ein Unternehmen mit der Entwicklung einer App beauftragt hat, als Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO angesehen werden kann, wenn die Stelle selbst keine Verarbeitungsvorgänge durchgeführt, keine ausdrückliche Einwilligung zur Durchführung der konkreten Verarbeitungsvorgänge einholt und die Anwendung nicht erworben hat. Dies wird durch das Gericht – unter Berücksichtigung der weiten Auslegung des Begriffs der Verantwortlichkeit[1] – bejaht.[2] In Fortschreibung seiner Rechtsprechung stellt das Gericht für die Beurteilung der Verantwortlichkeit auf das tatsächliche Eigeninteresse an der Verarbeitung sowie auf die Einflussmöglichkeit über die Bestimmung der Zwecke und Mittel der Datenverarbeitung ab.[3]

Die Nennung als Verantwortlicher in der Datenschutzinformation i. S. d. Art. 13 DSGVO sei nur erheblich, wenn sich eine

* Mehr über die Autoren erfahren Sie am Ende des Beitrags.

1 Zweck dieser Verantwortlichkeit ist die Zuordnung jeder Verarbeitung an einen Verantwortlichen, vgl. EDSA, Leitlinien 07/2020, Version 2.0, Rn. 10.

2 EuGH, 5. 12. 2023 – C-683/21, K&R 2024, 119 ff., Rn. 38.

3 EuGH, 5. 12. 2023 – C-683/21, K&R 2024, 119 ff., Rn. 31. Diese Abgrenzungsmerkmale finden sich auch in EuGH, 10. 7. 2018 – C-25/17, Rn. 68 – Zeugen Jehovas. Vgl. *Hartung*, in Kühling/Buchner, 4. Aufl. 2024, Art. 4 DSGVO, Nr. 7 Rn. 13 m. w. N. zur Bestimmung der Verantwortlichkeit.

ausdrückliche oder stillschweigende Zustimmung nachweisen ließe. Lediglich wenn das Gericht im Ausgangsverfahren einen ausdrücklichen Widerspruch des NZÖG gegen die Veröffentlichung der App hätte feststellen können, käme eine Verantwortlichkeit des NZÖG nicht in Betracht.

2. Gemeinsame Verantwortlichkeit ohne ausdrückliche Vereinbarung

Der Abschluss eines Joint-Controllership-Vertrags ist kein konstitutives Merkmal für das Bestehen einer gemeinsamen Verantwortlichkeit.[4] Aus der Pflicht des Verantwortlichen zum Abschluss eines Joint-Controllership-Vertrags aus Art. 26 Abs. 1 DSGVO i. V. m. dem 79. Erwägungsgrund der DSGVO resultiert im Umkehrschluss nicht, dass ohne eine solche Vereinbarung keine Verarbeitung in gemeinsamer Verantwortlichkeit angenommen werden kann. Für diese Auslegung spricht der Normwortlaut des Art. 26 Abs. 1 S. 2 DSGVO, der keine konstitutive Wirkung nahelegt, sowie der Sinn und Zweck der Abschlusspflicht eines Joint-Controllership-Vertrags. Dieser ist vordergründig auf eine Erfüllung der (Transparenz-) Pflichten gegenüber den Betroffenen gerichtet.[5]

3. Verwendung von Daten für IT-Tests als Verarbeitung

Die Verwendung (von Kopien) personenbezogener Daten für IT-Tests wird durch den EuGH als Verarbeitung i. S. d. Art. 4 Nr. 2 DSGVO qualifiziert.[6] Lediglich zur Klarstellung weist das Gericht darauf hin, dass anonymisierten oder fiktiven Daten der Personenbezug fehlt.

4. Bußgeld gegen den Verantwortlichen aufgrund eines DSGVO-Verstoßes des Auftragsverarbeiters

Der EuGH stellt zunächst das Erfordernis eines fahrlässigen oder vorsätzlichen Verstoßes durch den Verantwortlichen fest. Dieses Verschuldenserfordernis dürfe nach Auffassung des Gerichts auch nicht durch die Aufsichtsbehörden der Mitgliedsstaaten unterlaufen werden, da die materiellen Anforderungen zur Verhängung einer Geldbuße unmittelbar gälten. Die Aufsichtsbehörden müssten stets ein Verschulden des Verantwortlichen nachweisen.[7] Der gegenläufigen Auffassung, nach der der Aufsichtsbehörde ein gewisses Ermessen bei der Verhängung einer Geldbuße ohne Verschuldensnachweis zukommen soll,[8] erteilt der EuGH somit eine Absage.[9]

Der Verantwortliche haftet nach Art. 83 Abs. 3 DSGVO für eigene und für durch einen Auftragsverarbeiter im Namen des Verantwortlichen begangene Datenschutzverstöße. Zugleich nimmt das Gericht eine klare Beschränkung der Haftung des Verantwortlichen vor:

„Die Haftung des Verantwortlichen für das Verhalten eines Auftragsverarbeiters kann sich jedoch nicht auf Fälle erstrecken, in denen der Auftragsverarbeiter personenbezogene Daten für eigene Zwecke verarbeitet hat oder diese Daten auf eine Weise verarbeitet hat, die nicht mit dem Rahmen oder den Modalitäten der Verarbeitung, wie sie vom Verantwortlichen festgelegt wurden, vereinbar ist oder auf eine Weise, bei der vernünftigerweise nicht davon ausgegangen werden kann, dass der Verantwortliche ihr zugestimmt hätte."[10]

Deutlich wird dabei die klare Beschränkung der Befugnisse des Auftragsverarbeiters auf die ausdrücklichen oder konkludenten Abreden *inter partes*. Überschreitet der Auftragsverarbeiter die Grenzen dieser Abreden (sog. *Exzess des Auftragsverarbeiters*),[11] fingiert dies gem. Art. 28 Abs. 10 DSGVO die Behandlung des Auftragsverarbeiters als Verantwortlichen. Eine Bußgeldhaftung des Verantwortlichen für Verstöße des Auftragsverarbeiters kommt somit nur in Betracht, wenn kein Exzess des Auftragsverarbeiters vorliegt.

IV. Auswirkungen in der Praxis

Die Abgrenzung des EuGH zur Haftung des Verantwortlichen für Verstöße des Auftragsverarbeiters ist von großer Praxisrelevanz. Mit der Entscheidung wird im Wesentlichen die Beschränkung der Haftung auf die ausdrücklichen oder konkludenten Parteiabreden klargestellt. Für Verantwortliche und Auftragsverarbeiter folgt daraus gleichermaßen ein Gebot zu einer sorgfältigen Prüfung der Auftragsverarbeitungsverträge. Insbesondere der Verantwortliche sollte in eigenem Interesse sicherstellen, dass die Grenzen der Aufgaben des Auftragsverarbeiters klar abgesteckt sind. Konkret bedeutet dies: Die durchzuführende Auftragsverarbeitung ist konkret zu beschreiben – gemäß Art. 28 Abs. 3 S. 1 DSGVO betrifft dies den Gegenstand und die Dauer der Verarbeitung, die Art und den Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen. Nur so lässt sich, wenn nötig, ein Exzess des Auftragsverarbeiters präzise bestimmen, sodass eine Haftungsfreizeichnung des Verantwortlichen aufgrund der fingierten Haftung des Auftragsverarbeiters möglich wird.

Unter Berücksichtigung des Vorgenannten bleibt der Abschluss eines Auftragsverarbeitungsvertrags nicht nur gem. Art. 28 Abs. 3 DSGVO rechtlich vorgeschrieben, sondern auch unter Haftungsgesichtspunkten dringend geboten. Die vertragliche Fixierung des Auftragsinhaltes ermöglicht eine klare Begrenzung der Befugnisse des Auftragsverarbeiters.

Offen bleibt nach der Entscheidung des EuGH in diesem Zusammenhang, ob die fehlende konstitutive Wirkung eines Joint-Controllership-Vertrags auch auf Auftragsverarbeitungsverträge übertragbar ist. Ein gewichtiges Argument für eine konstitutive Wirkung des Auftragsverarbeitungsvertrags bildet die anders als bei dem Joint-Controllership enthaltene Formvorschrift (Art. 28 Abs. 9 DSGVO).[12]

Einen in der bisherigen Diskussion zur Abgrenzung unterschiedlicher Verantwortlichkeiten nicht aufgebrachten Aspekt bringt der EuGH nun ins Spiel. Im Hinblick auf die Beurteilung einer datenschutzrechtlichen Verantwortlichkeit weist der EuGH auf die Bedeutung von Aussagen in Datenschutzinformationen hin. So soll eine dortige Aussage, der Vertragspartner sei eigener Verantwortlicher bzw. gemeinsamer Verantwortlicher, im Falle einer Billigung durch das Unternehmen ein Indiz im Rahmen der Bewertung der Verantwortlichkeit sein. Relevant werden kann dies beispielsweise für Dienstleister, die als Auftragsverarbeiter tätig werden wollen, in Datenschutzformationen des Auftraggebers aber als (gemeinsamer) Verantwortlicher genannt werden. Ebenso könnte dies

4 EuGH, 5. 12. 2023 – C-683/21, K&R 2024, 119, Rn. 46. So auch *Hartung*, in Kühling/Buchner (Fn. 3), Art. 26 DSGVO, Rn. 52 m. w. N.
5 So auch *Bertermann*, in Ehmann/Selmayr, 2. Aufl. 2018, Art. 26 DSGVO, Rn. 12. Vgl. zum Verweis auf die Transparenzpflichten *Lang*, in: Taeger/Gabel, 4. Aufl. 2022, Art. 26 DSGVO, Rn. 95.
6 EuGH, 5. 12. 2023 – C-683/21, K&R 2024, 119 ff., Rn. 59.
7 Dies knüpft auch an die Parallelentscheidung des Gerichts zur Deutsche Wohnen SE, in der einer Haftung für lediglich objektive DSGVO-Verstöße („strict liability") eine Absage erteilt wurde, an, vgl. EuGH, 5. 12. 2023 – C-807/21, K&R 2024, 35, Rn. 78 m. Anm. *Grosmann/Hansen*.
8 Vgl. Schlussanträge des Generalanwalts, 4. 5. 2023 – C-683/21, Rn. 87 ff. m. w. N.
9 EuGH, 5. 12. 2023 – C-683/21, K&R 2024, 119 ff., Rn. 62. Zur Einordnung in das nationale Recht *Boehm*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 83 DSGVO, Rn. 25.
10 EuGH, 5. 12. 2023 – C-683/21, K&R 2024, 119 ff., Rn. 85.
11 Vgl. *Martini*, in: Paal/Pauly, 3. Aufl. 2021, Art. 28 DSGVO, Rn. 76 f.; *Petri*, in: Simitis/Hornung/Spiecker gen. Döhmann (Fn. 9), Art. 28 DSGVO, Rn. 94.
12 Vgl. *Gabel/Lutz*, in: Taeger/Gabel (Fn. 5), Art. 28 DSGVO, Rn. 72 m. w. N.

in einer Konstellation zum Problem werden, in der ein eigener Verantwortlicher in den Datenschutzinformationen des Vertragspartners als gemeinsamer Verantwortlicher genannt wird und dadurch möglicherweise den Anforderungen des Art. 26 DSGVO unterfällt.

Die Feststellung, dass auch die Verwendung personenbezogener Daten für IT-Tests als Verarbeitung zu qualifizieren ist, ist zunächst wenig überraschend. Diese Datenverarbeitungen können bei Einhaltung der Grundsätze des Art. 5 Abs. 1 DSGVO und bei Vorliegen eines überwiegenden berechtigten Interesses gem. Art. 6 Abs. 1 S. 1 lit. f DSGVO zulässig sein.

In der Praxis stellen sich darüber hinaus Abgrenzungsfragen, wenn IT-Dienstleister, die als Auftragsverarbeiter tätig sind, Informationen über das Nutzungsverhalten der User für (eigene) Analyse- und Softwareoptimierungszwecke nutzen. So ist bisher ungeklärt, ob diese Datenverarbeitungen noch von der Auftragsverarbeitung umfasst sind oder eine eigene Verantwortlichkeit des Dienstleisters begründen. Hiervon hängt ab, welche Rechtsgrundlage für die Datenverarbeitung erforderlich ist und wen Informations- und Auskunftspflichten treffen.

Dr. Patrick Grosmann

Rechtsanwalt bei der Kanzlei FPS PartG mbB in Frankfurt a. M., Studium der Rechts- & Politikwissenschaft (M.A.). Promotion zu den Interessenkonflikten der Datenschutzbeauftragten. Zertifizierter Datenschutzbeauftragter (TÜV®), Datenschutz-Auditor (DGI®) und Dozent für Datenschutzbeauftragte. Er berät Unternehmen im Datenschutz- und IT-Recht.

Dr. Hauke Hansen

Partner der Kanzlei FPS PartG mbB an ihrem Frankfurter Standort, zertifizierter Datenschutzbeauftragter (TÜV®), Fachanwalt für IT-Recht und Lehrbeauftragter der Goethe-Universität Frankfurt a. M. Seit 20 Jahren berät er Unternehmen im Datenschutzrecht, im Zusammenhang mit IT Security und der Digitalisierung ihrer Tätigkeiten.

Rechtsprechung

Geeignete technische und organisatorische Maßnahmen bei Cyberangriff

EuGH, Urteil vom 14. 12. 2023 – C-340/21

Volltext-ID: KuRL2024-104, www.kommunikationundrecht.de

VB ./. Natsionalna agentsia za prihodite

ECLI:EU:C:2023:986

Verfahrensgang: Varhoven administrativen sad (Oberstes VG, Bulgarien), 14. 5. 2021

Art. 5, 24, 32, 82 VO (EU) 2016/679

1. Die Art. 24 und 32 der VO (EU) 2016/679 […] sind dahin auszulegen, dass eine unbefugte Offenlegung von bzw. ein unbefugter Zugang zu personenbezogenen Daten durch „Dritte" im Sinne von Art. 4 Nr. 10 dieser Verordnung allein nicht ausreicht, um anzunehmen, dass die technischen und organisatorischen Maßnahmen, die der für die betreffende Verarbeitung Verantwortliche getroffen hat, nicht „geeignet" im Sinne der Art. 24 und 32 dieser Verordnung waren.

2. Art. 32 der VO 2016/679 ist dahin auszulegen, dass die Geeignetheit der vom Verantwortlichen nach diesem Artikel getroffenen technischen und organisatorischen Maßnahmen von den nationalen Gerichten konkret zu beurteilen ist, wobei die mit der betreffenden Verarbeitung verbundenen Risiken zu berücksichtigen sind und zu beurteilen ist, ob Art, Inhalt und Umsetzung dieser Maßnahmen diesen Risiken angemessen sind.

3. Der in Art. 5 Abs. 2 der VO 2016/679 formulierte und in Art. 24 dieser Verordnung konkretisierte Grundsatz der Rechenschaftspflicht des Verantwortlichen ist dahin auszulegen, dass im Rahmen einer auf Art. 82 der Verordnung gestützten Schadenersatzklage der für die betreffende Verarbeitung Verantwortliche die Beweislast dafür trägt, dass die von ihm getroffenen Sicherheitsmaßnahmen im Sinne von Art. 32 dieser Verordnung geeignet waren.

4. Art. 32 der VO 2016/679 und der unionsrechtliche Effektivitätsgrundsatz sind dahin auszulegen, dass für die Beurteilung der Geeignetheit der Sicherheitsmaßnahmen, die der Verantwortliche nach diesem Artikel getroffen hat, ein gerichtliches Sachverständigengutachten kein generell notwendiges und ausreichendes Beweismittel sein kann.

5. Art. 82 Abs. 3 der VO 2016/679 ist dahin auszulegen, dass der Verantwortliche von seiner nach Art. 82 Abs. 1 und 2 dieser Verordnung bestehenden Pflicht zum Ersatz des einer Person entstandenen Schadens nicht allein deshalb befreit werden kann, weil dieser Schaden die Folge einer unbefugten Offenlegung von bzw. eines unbefugten Zugangs zu personenbezogenen Daten durch „Dritte" im Sinne von Art. 4 Nr. 10 dieser Verordnung ist, wobei der Verantwortliche dann nachweisen muss, dass er in keinerlei Hinsicht für den Umstand, durch den der betreffende Schaden eingetreten ist, verantwortlich ist.

6. Art. 82 Abs. 1 der VO 2016/679 ist dahin auszulegen, dass allein der Umstand, dass eine betroffene Person infolge eines Verstoßes gegen diese Verordnung befürchtet, dass ihre personenbezogenen Daten durch Dritte missbräuchlich verwendet werden könnten, einen „immateriellen Schaden" im Sinne dieser Bestimmung darstellen kann. (Tenor des Gerichts)

Sachverhalt

Das Vorabentscheidungsersuchen betrifft die Auslegung von Art. 5 Abs. 2, den Art. 24 und 32 sowie Art. 82 Abs. 1 bis 3 der VO (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. 4. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG (Datenschutz-Grundverordnung) (ABl. 2016, L 119, S. 1, im Folgenden: DSGVO).

Es ergeht im Rahmen eines Rechtsstreits zwischen VB, einer natürlichen Person, und der Natsionalna agentsia za prihodite (Nationale Agentur für Einnahmen, Bulgarien) (im Folgenden: NAP) über den Ersatz des immateriellen Schadens, der dieser Person dadurch entstanden sein soll, dass diese Behörde ihre gesetzlichen Verpflichtungen als für die Verarbeitung personenbezogener Daten Verantwortliche verletzt haben soll.