# Kommunikation & Recht

K&R

2 | Februar 2024
27. Jahrgang
Seiten 85 - 156



www.kommunikationundrecht.de

dfv Mediengruppe
Frankfurt am Main

Trilog-Einigung zum VO-Vorschlag politische Werbung
**Dr. Daniel Holznagel**

**85** Haftungsrisiken beim Einsatz von Open-Source-Software in der Supply Chain von Unternehmen
**Prof. Dr. Felix Buchmann, André Fritsche und Sebastian Nardone**

**93** § 327p Abs.1 S. 2 BGB – Systemsprenger oder maßvolle Weiterentwicklung?
**Prof. Dr. Tabea Bauermeister**

**98** AGB-Kontrolle von Datenschutzhinweisen und Drittlandtransfer an Google
**Susanne Klein**

**102** Neues zur Haftung von Auftragsverarbeitern und Verantwortlichen
**Dr. Patrick Grosmann und Dr. Hauke Hansen**

**104** **EuGH:** Geeignete technische und organisatorische Maßnahmen bei Cyberangriff
mit Kommentar von **Peter Hense**

**112** **EuGH:** Nachweispflicht bei Schadensersatz wegen Datenschutzverstoß

**114** **EuGH:** Schadensersatz wegen rechtswidriger Verarbeitung von Gesundheitsdaten

**119** **EuGH:** Verantwortliche bei staatlich beauftragter Pandemie-App

**124** **BGH:** Zulässige identifizierende Tatschilderung einer Sexualstraftat

**130** **OLG Köln:** ddl-music.to: Urheberrechtsverletzung durch Content-Delivery-Network
mit Kommentar von **Robert Golz**

**138** **OLG Köln:** Minderung schließt Sonderkündigung bei mangelhaftem Internet nicht aus
mit Kommentar von **Dr. Gerd Kiparski**

**142** **KG Berlin:** Unwirksame AGB zu Preisanpassung bei Streaming-Abo

**150** **VG Köln:** Identifizierende Pressemitteilung der BNetzA zu Bußgeld unzulässig
mit Kommentar von **Dr. Fiete Kalscheuer**

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.

Die NAP ist eine dem bulgarischen Finanzminister unterstellte Behörde. Im Rahmen ihrer Aufgaben, die u. a. in der Feststellung, Sicherung und Einziehung öffentlicher Forderungen bestehen, ist sie für die Verarbeitung personenbezogener Daten verantwortlich im Sinne von Art. 4 Nr. 7 DSGVO.

Am 15. 7. 2019 wurde in den Medien darüber berichtet, dass ein unbefugter Zugang zum IT-System der NAP erfolgt sei und dass infolge dieses Cyberangriffs in diesem System enthaltene personenbezogene Daten im Internet veröffentlicht worden seien.

Mehr als sechs Millionen natürliche Personen, zu denen sowohl bulgarische als auch ausländische Staatsbürger zählten, waren von diesen Ereignissen betroffen. Einige Hundert von ihnen, darunter die Klägerin des Ausgangsverfahrens, verklagten die NAP auf Ersatz des immateriellen Schadens, der sich aus der Offenlegung ihrer personenbezogenen Daten ergeben haben soll.

Vor diesem Hintergrund erhob die Klägerin des Ausgangsverfahrens beim Administrativen sad Sofia-grad (VG der Stadt Sofia, Bulgarien) auf der Grundlage von Art. 82 DSGVO und Bestimmungen des bulgarischen Rechts Klage auf Verurteilung der NAP zur Zahlung von 1000 bulgarischen Lew (BGN) (etwa 510 Euro) an sie als Schadenersatz. Zur Stützung dieses Antrags machte sie geltend, sie habe einen immateriellen Schaden erlitten, der sich aus einer Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO und insbesondere aus einer Verletzung der Sicherheit ergebe, die dadurch verursacht worden sei, dass die NAP gegen ihre Verpflichtungen insbesondere aus Art. 5 Abs. 1 lit. f sowie den Art. 24 und 32 DSGVO verstoßen habe. Ihr immaterieller Schaden bestehe in der Befürchtung, dass ihre personenbezogenen Daten, die ohne ihre Einwilligung veröffentlicht worden seien, künftig missbräuchlich verwendet würden oder dass sie selbst erpresst, angegriffen oder sogar entführt werde.

Mit Entscheidung vom 27. 11. 2020 wies der Administrativen sad Sofia-grad (VG der Stadt Sofia) die Klage der Klägerin des Ausgangsverfahrens ab.

Die Klägerin des Ausgangsverfahrens legte gegen diese Entscheidung Kassationsbeschwerde beim Varhoven administrativen sad (Oberstes VG, Bulgarien), dem vorlegenden Gericht in der vorliegenden Rechtssache, ein.

## Zu den Vorlagefragen

*Zur ersten Frage*

***22*** Mit seiner ersten Frage möchte das vorlegende Gericht im Wesentlichen wissen, ob die Art. 24 und 32 DSGVO dahin auszulegen sind, dass eine unbefugte Offenlegung von bzw. ein unbefugter Zugang zu personenbezogenen Daten durch „Dritte“ im Sinne von Art. 4 Nr. 10 DSGVO allein 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 DSGVO waren.

***23*** Zunächst ist darauf hinzuweisen, dass nach ständiger Rechtsprechung die Begriffe einer Bestimmung des Unionsrechts, die – wie die Art. 24 und 32 DSGVO – für die Ermittlung ihres Sinns und ihrer Tragweite nicht ausdrücklich auf das Recht der Mitgliedstaaten verweist, in der Regel in der gesamten Union eine autonome und einheitliche Auslegung erhalten müssen, die insbesondere unter Berücksichtigung des Wortlauts der betreffenden Bestimmung, der mit ihr verfolgten Ziele und des Zusammenhangs, in den sie sich einfügt, zu ermitteln ist (vgl. in diesem Sinne Urteile vom 18. 1. 1984, Ekro, 327/82, EU:C:1984:11, Rn. 11, vom 1. 10. 2019, Planet49, C-673/17, [K&R 2019, 705 ff. =] EU:C:2019:801, Rn. 47 und 48, sowie vom 4. 5. 2023, Österreichische Post [Immaterieller Schaden im Zusammenhang mit der Verarbeitung personenbezogener Daten], C-300/21, [K&R 2023, 416 ff. =] EU:C:2023:370, Rn. 29).

***24*** Erstens ist zum Wortlaut der einschlägigen Bestimmungen festzustellen, dass Art. 24 DSGVO eine allgemeine Verpflichtung des für die Verarbeitung personenbezogener Daten Verantwortlichen vorsieht, geeignete technische und organisatorische Maßnahmen umzusetzen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß der DSGVO erfolgt.

***25*** Hierzu führt Art. 24 Abs. 1 DSGVO eine Reihe von Kriterien auf, die für die Beurteilung der Geeignetheit solcher Maßnahmen zu berücksichtigen sind, nämlich Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen. Weiter heißt es dort, dass diese Maßnahmen erforderlichenfalls überprüft und aktualisiert werden.

***26*** Vor diesem Hintergrund legt Art. 32 DSGVO die Pflichten des Verantwortlichen und eines etwaigen Auftragsverarbeiters in Bezug auf die Sicherheit dieser Verarbeitung fest. So bestimmt Art. 32 Abs. 1 DSGVO, dass diese unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der betreffenden Verarbeitung geeignete technische und organisatorische Maßnahmen treffen, um ein Schutzniveau zu gewährleisten, das den in der vorstehenden Randnummer des vorliegenden Urteils genannten Risiken angemessen ist.

***27*** Ebenso sind nach Art. 32 Abs. 2 DSGVO bei der Beurteilung des angemessenen Schutzniveaus insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von bzw. unbefugten Zugang zu personenbezogenen Daten.

***28*** Zudem heißt es sowohl in Art. 24 Abs. 3 DSGVO als auch in Art. 32 Abs. 3 DSGVO, dass der Verantwortliche oder der Auftragsverarbeiter die Erfüllung der in den jeweiligen Abs. 1 dieser Artikel genannten Anforderungen nachweisen kann, indem er sich auf die Einhaltung genehmigter Verhaltensregeln bzw. eines genehmigten Zertifizierungsverfahrens gemäß Art. 40 bzw. Art. 42 DSGVO stützt.

***29*** Die Bezugnahme in Art. 32 Abs. 1 und 2 DSGVO auf „ein dem Risiko angemessenes Schutzniveau“ und ein „angemessenes Schutzniveau“ zeigt, dass mit der DSGVO ein Risikomanagementsystem eingeführt und in ihr in keiner Weise behauptet wird, dass sie das Risiko von Verletzungen des Schutzes personenbezogener Daten beseitigt.

***30*** Somit ergibt sich aus dem Wortlaut der Art. 24 und 32 DSGVO, dass diese Bestimmungen dem Verantwortlichen lediglich vorschreiben, technische und organisatorische Maßnahmen zu treffen, die darauf gerichtet sind, jede Verletzung des Schutzes personenbezogener Daten so weit wie möglich zu verhindern. Die Geeignetheit solcher Maßnahmen ist konkret zu bewerten, indem geprüft wird, ob der Verantwortliche diese Maßnahmen unter Berücksichtigung der verschiedenen in den genannten Artikeln aufgeführten Kriterien und der Datenschutzbedürfnisse getroffen hat, die speziell mit der betreffenden Verarbeitung sowie den davon ausgehenden Risiken verbunden sind.

**31** Folglich können die Art. 24 und 32 DSGVO nicht dahin verstanden werden, dass eine unbefugte Offenlegung von bzw. ein unbefugter Zugang zu personenbezogenen Daten durch einen Dritten für die Schlussfolgerung ausreicht, dass die von dem für die betreffende Verarbeitung Verantwortlichen ergriffenen Maßnahmen nicht im Sinne dieser Bestimmungen geeignet waren, ohne dass ihm die Möglichkeit eingeräumt wird, den Gegenbeweis zu erbringen.

**32** Eine solche Auslegung ist umso mehr geboten, als Art. 24 DSGVO ausdrücklich vorsieht, dass der Verantwortliche den Nachweis dafür erbringen können muss, dass die von ihm umgesetzten Maßnahmen im Einklang mit der DSGVO stehen; diese Möglichkeit bliebe ihm verwehrt, wenn eine unwiderlegbare Vermutung angenommen würde.

**33** Zweitens bestätigen systematische und teleologische Gesichtspunkte diese Auslegung der Art. 24 und 32 DSGVO.

**34** Was zum einen den Zusammenhang betrifft, in den sich diese beiden Artikel einfügen, ist darauf hinzuweisen, dass sich aus Art. 5 Abs. 2 DSGVO ergibt, dass der Verantwortliche nachweisen können muss, dass er die in Abs. 1 dieses Artikels genannten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten hat. Diese Verpflichtung wird in Art. 24 Abs. 1 und 3 sowie in Art. 32 Abs. 3 DSGVO hinsichtlich der Verpflichtung, technische und organisatorische Maßnahmen zum Schutz solcher Daten bei der Verarbeitung durch den Verantwortlichen zu treffen, aufgegriffen und präzisiert. Eine solche Verpflichtung, die Geeignetheit der Maßnahmen nachzuweisen, hätte indes keinen Sinn, wenn der Verantwortliche verpflichtet wäre, jede Beeinträchtigung dieser Daten zu verhindern.

**35** Zudem sollte der Verantwortliche nach dem 74. Erwägungsgrund der DSGVO geeignete und wirksame Maßnahmen treffen müssen und nachweisen können, dass die Verarbeitungstätigkeiten im Einklang mit der DSGVO stehen und die Maßnahmen auch wirksam sind, wobei er die Kriterien berücksichtigen sollte, die mit den ebenfalls in den Art. 24 und 32 DSGVO genannten Merkmalen der betreffenden Verarbeitung und dem von ihr ausgehenden Risiko zusammenhängen.

**36** Nach dem 76. Erwägungsgrund der DSGVO hängen außerdem Eintrittswahrscheinlichkeit und Schwere des Risikos von den Besonderheiten der betreffenden Verarbeitung ab und sollte dieses Risiko anhand einer objektiven Bewertung beurteilt werden.

**37** Darüber hinaus ergibt sich aus Art. 82 Abs. 2 und 3 DSGVO, dass ein Verantwortlicher zwar für den Schaden haftet, der durch eine nicht der DSGVO entsprechende Verarbeitung verursacht wurde, er jedoch von seiner Haftung befreit wird, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

**38** Zum anderen wird die in Rn. 31 des vorliegenden Urteils vorgenommene Auslegung auch durch den 83. Erwägungsgrund der DSGVO bestätigt, in dessen S. 1 es heißt: „Zur Aufrechterhaltung der Sicherheit und zur Vorbeugung gegen eine gegen diese Verordnung verstoßende Verarbeitung sollte der Verantwortliche oder der Auftragsverarbeiter die mit der Verarbeitung verbundenen Risiken ermitteln und Maßnahmen zu ihrer Eindämmung … treffen." Damit hat der Unionsgesetzgeber seine Absicht zum Ausdruck gebracht, die Risiken einer Verletzung des Schutzes personenbezogener Daten „einzudämmen", ohne zu behaupten, dass sie beseitigt werden könnten.

**39** Nach alledem ist auf die erste Frage [wie im Tenor, Punkt 1] zu antworten […]

*Zur zweiten Frage*

**40** Mit seiner zweiten Frage möchte das vorlegende Gericht im Wesentlichen wissen, ob Art. 32 DSGVO dahin auszulegen ist, dass die Geeignetheit der vom Verantwortlichen nach diesem Artikel getroffenen technischen und organisatorischen Maßnahmen von den nationalen Gerichten konkret, insbesondere unter Berücksichtigung der mit der betreffenden Verarbeitung verbundenen Risiken, zu beurteilen ist.

**41** Insoweit ist darauf hinzuweisen, dass, wie im Rahmen der Beantwortung der ersten Frage ausgeführt wurde, Art. 32 DSGVO verlangt, dass, je nach Sachverhalt, der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen treffen, um unter Berücksichtigung der in Art. 32 Abs. 1 DSGVO genannten Beurteilungskriterien ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Zudem zählt Art. 32 Abs. 2 DSGVO in nicht abschließender Weise eine Reihe von Kriterien auf, die für die Bewertung des angemessenen Schutzniveaus im Hinblick auf die mit der betreffenden Verarbeitung verbundenen Risiken relevant sind.

**42** Aus Art. 32 Abs. 1 und 2 DSGVO ergibt sich, dass die Geeignetheit solcher technischen und organisatorischen Maßnahmen in zwei Schritten zu beurteilen ist. Zum einen sind die von der betreffenden Verarbeitung ausgehenden Risiken einer Verletzung des Schutzes personenbezogener Daten und ihre möglichen Folgen für die Rechte und Freiheiten natürlicher Personen zu ermitteln. Diese Beurteilung muss konkret unter Berücksichtigung der Eintrittswahrscheinlichkeit und Schwere der ermittelten Risiken erfolgen. Zum anderen ist zu prüfen, ob die vom Verantwortlichen getroffenen Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke dieser Verarbeitung diesen Risiken angemessen sind.

**43** Zwar verfügt der Verantwortliche über einen gewissen Entscheidungsspielraum bei der Festlegung geeigneter technischer und organisatorischer Maßnahmen, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten, wie es Art. 32 Abs. 1 DSGVO verlangt. Gleichwohl muss ein nationales Gericht die komplexe Beurteilung, die der Verantwortliche vorgenommen hat, bewerten können und sich dabei vergewissern können, dass die vom Verantwortlichen gewählten Maßnahmen geeignet sind, ein solches Sicherheitsniveau zu gewährleisten.

**44** Eine solche Auslegung ist im Übrigen geeignet, zum einen die Wirksamkeit des Schutzes personenbezogener Daten, die in den Erwägungsgründen 11 und 74 der DSGVO hervorgehoben wird, und zum anderen das durch Art. 79 Abs. 1 i. V. m. dem vierten Erwägungsgrund der DSGVO geschützte Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche zu gewährleisten.

**45** Daher darf sich ein nationales Gericht bei der Kontrolle der Geeignetheit der nach Art. 32 DSGVO getroffenen technischen und organisatorischen Maßnahmen nicht auf die Feststellung beschränken, in welcher Weise der für die betreffende Verarbeitung Verantwortliche seinen Verpflichtungen aus diesem Artikel nachkommen wollte, sondern muss eine materielle Prüfung dieser Maßnahmen anhand aller in diesem Artikel genannten Kriterien sowie der Umstände des Einzelfalls und der dem Gericht dafür zur Verfügung stehenden Beweismittel vornehmen.

**46** Eine solche Prüfung erfordert eine konkrete Untersuchung sowohl der Art als auch des Inhalts der vom Verantwortlichen getroffenen Maßnahmen, der Art und Weise, in der diese Maßnahmen angewandt wurden, und ihrer praktischen Auswirkungen auf das Sicherheitsniveau, das der Verantwortliche

in Anbetracht der mit dieser Verarbeitung verbundenen Risiken zu gewährleisten hatte.

**47** Daher ist auf die zweite Frage [wie im Tenor, Punkt 2] zu antworten […]

*Zur dritten Frage*

Zum ersten Teil der dritten Frage

**48** Mit dem ersten Teil seiner dritten Frage möchte das vorlegende Gericht im Wesentlichen wissen, ob der in Art. 5 Abs. 2 DSGVO formulierte und in Art. 24 DSGVO konkretisierte Grundsatz der Rechenschaftspflicht des Verantwortlichen dahin auszulegen ist, dass im Rahmen einer auf Art. 82 DSGVO gestützten Schadenersatzklage der für die betreffende Verarbeitung Verantwortliche die Beweislast dafür trägt, dass die von ihm getroffenen Sicherheitsmaßnahmen im Sinne von Art. 32 DSGVO geeignet waren.

**49** In diesem Zusammenhang ist erstens darauf hinzuweisen, dass Art. 5 Abs. 2 DSGVO einen Grundsatz der Rechenschaftspflicht aufstellt, nach dem der Verantwortliche für die Einhaltung der in Art. 5 Abs. 1 DSGVO niedergelegten Grundsätze für die Verarbeitung personenbezogener Daten verantwortlich ist, und der vorsieht, dass dieser Verantwortliche nachweisen können muss, dass diese Grundsätze eingehalten werden.

**50** Insbesondere muss der Verantwortliche gemäß dem Grundsatz der Integrität und Vertraulichkeit personenbezogener Daten, der in Art. 5 Abs. 1 lit. f DSGVO festgelegt ist, sicherstellen, dass solche Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit der Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen, und er muss nachweisen können, dass dieser Grundsatz beachtet wird.

**51** Ferner ist darauf hinzuweisen, dass sowohl Art. 24 Abs. 1 i. V. m. dem 74. Erwägungsgrund der DSGVO als auch Art. 32 Abs. 1 DSGVO den Verantwortlichen verpflichten, in Bezug auf jedwede Verarbeitung personenbezogener Daten, die durch ihn oder in seinem Namen erfolgt, geeignete technische und organisatorische Maßnahmen umzusetzen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß der DSGVO erfolgt.

**52** Aus dem Wortlaut von Art. 5 Abs. 2, Art. 24 Abs. 1 und Art. 32 Abs. 1 DSGVO geht eindeutig hervor, dass die Beweislast dafür, dass personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit dieser Daten im Sinne von Art. 5 Abs. 1 lit. f und Art. 32 DSGVO gewährleistet, dem für die betreffende Verarbeitung Verantwortlichen obliegt (vgl. entsprechend Urteile vom 4. 5. 2023, Bundesrepublik Deutschland [Elektronisches Gerichtsfach], C-60/22, EU:C:2023:373, Rn. 52 und 53, und vom 4. 7. 2023, Meta Platforms u. a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, [K&R 2023, 492 ff. =] EU:C:2023:537, Rn. 95).

**53** Diese drei Artikel formulieren somit eine allgemein anwendbare Regel, die mangels gegenteiliger Anhaltspunkte in der DSGVO auch im Rahmen einer auf Art. 82 DSGVO gestützten Schadenersatzklage anzuwenden ist.

**54** Zweitens ist festzustellen, dass die vorstehende wörtliche Auslegung bestätigt wird, wenn man die mit der DSGVO verfolgten Ziele berücksichtigt.

**55** Da zum einen das von der DSGVO angestrebte Schutzniveau von den Sicherheitsmaßnahmen abhängt, die von den für die Verarbeitung dieser Daten Verantwortlichen getroffen werden, müssen diese – mittels der ihnen obliegenden Beweislast für die Geeignetheit dieser Maßnahmen – dazu angehalten werden, alles zu unternehmen, um Verarbeitungsvorgänge zu verhindern, die nicht im Einklang mit der DSGVO stehen.

**56** Läge zum anderen die Beweislast für die Geeignetheit dieser Maßnahmen bei den betroffenen Personen im Sinne von Art. 4 Nr. 1 DSGVO, folgte daraus, dass dem in Art. 82 Abs. 1 DSGVO vorgesehenen Schadenersatzanspruch ein erheblicher Teil seiner praktischen Wirksamkeit genommen würde, obwohl der Unionsgesetzgeber, wie aus dem elften Erwägungsgrund der DSGVO hervorgeht, im Vergleich zu den vor Erlass der DSGVO geltenden Bestimmungen sowohl die Rechte dieser Personen stärken als auch die Verpflichtungen der Verantwortlichen verschärfen wollte.

**57** Daher ist auf den ersten Teil der dritten Frage [wie im Tenor, Punkt 3] zu antworten […]

Zum zweiten Teil der dritten Frage

**58** Mit dem zweiten Teil seiner dritten Frage möchte das vorlegende Gericht im Wesentlichen wissen, ob Art. 32 DSGVO und der unionsrechtliche Effektivitätsgrundsatz dahin auszulegen sind, dass für die Beurteilung der Geeignetheit der Sicherheitsmaßnahmen, die der Verantwortliche nach diesem Artikel getroffen hat, ein gerichtliches Sachverständigengutachten ein notwendiges und ausreichendes Beweismittel ist.

**59** Insoweit ist darauf hinzuweisen, dass es nach ständiger Rechtsprechung mangels einschlägiger Unionsregeln nach dem Grundsatz der Verfahrensautonomie Sache der innerstaatlichen Rechtsordnung jedes Mitgliedstaats ist, die verfahrensrechtlichen Modalitäten der Rechtsbehelfe, die zum Schutz der Rechte der Bürger bestimmt sind, festzulegen, vorausgesetzt allerdings, dass diese Modalitäten bei unter das Unionsrecht fallenden Sachverhalten nicht ungünstiger sind als diejenigen, die gleichartige Sachverhalte regeln, die dem innerstaatlichen Recht unterliegen (Äquivalenzgrundsatz), und dass sie die Ausübung der durch das Unionsrecht verliehenen Rechte nicht praktisch unmöglich machen oder übermäßig erschweren (Effektivitätsgrundsatz) (Urt. v. 4. 5. 2023, Österreichische Post [Immaterieller Schaden im Zusammenhang mit der Verarbeitung personenbezogener Daten], C-300/21, [K&R 2023, 416 ff. =] EU:C:2023:370, Rn. 53 und die dort angeführte Rechtsprechung).

**60** Im vorliegenden Fall ist festzustellen, dass die DSGVO keine Regeln über die Zulassung und den Beweiswert eines Beweismittels wie eines gerichtlichen Sachverständigengutachtens enthält, die von den nationalen Gerichten anzuwenden sind, die mit einer auf Art. 82 DSGVO gestützten Schadenersatzklage befasst sind und die Geeignetheit der von dem für die betreffende Verarbeitung Verantwortlichen getroffenen Sicherheitsmaßnahmen im Hinblick auf Art. 32 DSGVO zu beurteilen haben. Daher ist es nach den Ausführungen in der vorstehenden Randnummer des vorliegenden Urteils und in Ermangelung einschlägiger unionsrechtlicher Vorschriften Aufgabe der innerstaatlichen Rechtsordnung des einzelnen Mitgliedstaats, die Ausgestaltung von Klageverfahren, die den Schutz der dem Einzelnen aus Art. 82 DSGVO erwachsenden Rechte gewährleisten sollen, und insbesondere die Regeln für die Beweismittel, anhand deren die Geeignetheit solcher Maßnahmen in diesem Zusammenhang bewertet werden kann, festzulegen, wobei der Äquivalenz- und der Effektivitätsgrundsatz zu beachten sind (vgl. entsprechend Urteile vom 21. 6. 2022, Ligue des droits humains, C-817/19, [K&R 2022, 592 ff. =] EU:C:2022:491, Rn. 297, und vom 4. 5. 2023, Österreichische Post [Immaterieller Schaden im Zusammenhang mit der Verarbeitung personenbezogener Daten], C-300/21, [K&R 2023, 416 ff. =] EU:C:2023:370, Rn. 54).

**61** Im vorliegenden Verfahren hat der Gerichtshof keinen Anhaltspunkt für Zweifel an der Beachtung des Äquivalenzgrundsatzes. Etwas anderes gilt für die Vereinbarkeit mit dem Effektivitätsgrundsatz, da schon der Wortlaut des zweiten Teils der dritten Frage die Einholung eines gerichtlichen Sachverständigengutachtens als „notwendiges und ausreichendes Beweismittel" darstellt.

**62** Insbesondere könnte eine nationale Verfahrensvorschrift, nach der es generell „notwendig" wäre, dass die nationalen Gerichte ein gerichtliches Sachverständigengutachten anordnen, gegen den Effektivitätsgrundsatz verstoßen. Ein genereller Rückgriff auf ein solches Gutachten kann sich nämlich in Anbetracht anderer Beweise, die dem angerufenen Gericht vorliegen, als überflüssig erweisen; wie die bulgarische Regierung in ihren schriftlichen Erklärungen ausgeführt hat, gilt dies insbesondere im Hinblick auf Ergebnisse einer Kontrolle der Einhaltung der Maßnahmen zum Schutz personenbezogener Daten, die von einer unabhängigen und gesetzlich eingerichteten Behörde durchgeführt wurde, sofern diese Kontrolle erst kürzlich stattgefunden hat, da diese Maßnahmen gemäß Art. 24 Abs. 1 DSGVO erforderlichenfalls zu überprüfen und zu aktualisieren sind.

**63** Zudem könnte, wie die Europäische Kommission in ihren schriftlichen Erklärungen ausgeführt hat, der Effektivitätsgrundsatz verletzt sein, wenn der Begriff „ausreichend" dahin zu verstehen wäre, dass ein nationales Gericht ausschließlich oder automatisch aus einem gerichtlichen Sachverständigengutachten abzuleiten hätte, dass die von dem für die betreffende Verarbeitung Verantwortlichen getroffenen Sicherheitsmaßnahmen „geeignet" im Sinne von Art. 32 DSGVO sind. Die Wahrung der durch diese Verordnung eingeräumten Rechte, die mit dem Effektivitätsgrundsatz bezweckt wird, und insbesondere das durch Art. 79 Abs. 1 DSGVO garantierte Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen den Verantwortlichen erfordern indes, dass ein unparteiisches Gericht eine objektive Beurteilung der Geeignetheit der betreffenden Maßnahmen vornimmt, anstatt sich auf eine solche Ableitung zu beschränken (vgl. in diesem Sinne Urt. v. 12. 1. 2023, Nemzeti Adatvédelmi és Információszabadság Hatóság, C-132/21, [K&R 2023, 192 ff. =] EU:C:2023:2, Rn. 50).

**64** Nach alledem ist auf den zweiten Teil der dritten Frage [wie im Tenor, Punkt 4] zu antworten […]

*Zur vierten Frage*

**65** Mit seiner vierten Frage möchte das vorlegende Gericht im Wesentlichen wissen, ob Art. 82 Abs. 3 DSGVO dahin auszulegen ist, dass der Verantwortliche von seiner nach Art. 82 Abs. 1 und 2 DSGVO bestehenden Pflicht zum Ersatz des einer Person entstandenen Schadens allein deshalb befreit ist, 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 DSGVO ist.

**66** Zunächst ist klarzustellen, dass sich aus Art. 4 Nr. 10 DSGVO ergibt, dass „Dritte" insbesondere andere Personen sind als diejenigen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten. Diese Definition umfasst Personen wie die in der Vorlagefrage genannten, die keine Bediensteten des Verantwortlichen sind und nicht von diesem kontrolliert werden.

**67** Sodann ist erstens darauf hinzuweisen, dass nach Art. 82 Abs. 2 DSGVO „[j]eder an einer Verarbeitung beteiligte Verantwortliche … für den Schaden [haftet], der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde", und nach Art. 82 Abs. 3 DSGVO der Verantwortliche oder, je nach Sachverhalt, der Auftragsverarbeiter von dieser Haftung befreit wird, „wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist".

**68** Zudem heißt es in den ersten beiden Sätzen des 146. Erwägungsgrundes der DSGVO, der sich speziell auf Art. 82 DSGVO bezieht: „Der Verantwortliche oder der Auftragsverarbeiter sollte Schäden, die einer Person aufgrund einer Verarbeitung entstehen, die mit dieser Verordnung nicht im Einklang steht, ersetzen" und „von seiner Haftung befreit werden, wenn er nachweist, dass er in keiner Weise für den Schaden verantwortlich ist".

**69** Aus diesen Bestimmungen ergibt sich zum einen, dass der für die betreffende Verarbeitung Verantwortliche grundsätzlich einen Schaden ersetzen muss, der durch einen mit dieser Verarbeitung im Zusammenhang stehenden Verstoß gegen die DSGVO verursacht wurde, und zum anderen, dass er nur dann von seiner Haftung befreit werden kann, wenn er den Nachweis erbringt, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

**70** Wie die ausdrückliche Hinzufügung des Ausdrucks „in keinerlei Hinsicht" im Lauf des Gesetzgebungsverfahrens zeigt, müssen die Umstände, unter denen der Verantwortliche von der ihm nach Art. 82 DSGVO drohenden zivilrechtlichen Haftung befreit werden kann, streng auf solche beschränkt werden, unter denen der Verantwortliche nachweisen kann, dass er selbst nicht für den Schaden verantwortlich ist.

**71** Wenn, wie im vorliegenden Fall, eine Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO von Cyberkriminellen und damit von „Dritten" im Sinne von Art. 4 Nr. 10 DSGVO begangen wurde, kann diese Verletzung dem Verantwortlichen nur dann zugerechnet werden, wenn dieser die Verletzung unter Missachtung einer Verpflichtung aus der DSGVO, insbesondere der Verpflichtung zum Datenschutz, die ihm nach Art. 5 Abs. 1 lit. f, Art. 24 und Art. 32 DSGVO obliegt, ermöglicht hat.

**72** Somit kann sich der Verantwortliche bei einer Verletzung des Schutzes personenbezogener Daten durch einen Dritten auf der Grundlage von Art. 82 Abs. 3 DSGVO von seiner Haftung befreien, indem er nachweist, dass es keinen Kausalzusammenhang zwischen der etwaigen Verletzung der Verpflichtung zum Datenschutz durch ihn und dem der natürlichen Person entstandenen Schaden gibt.

**73** Zweitens steht die vorstehende Auslegung von Art. 82 Abs. 3 DSGVO auch im Einklang mit dem in den Erwägungsgründen 10 und 11 der DSGVO formulierten Ziel der DSGVO, ein hohes Schutzniveau für natürliche Personen bei der Verarbeitung ihrer personenbezogenen Daten zu gewährleisten.

**74** Nach alledem ist auf die vierte Frage [wie im Tenor, Punkt 5] zu antworten […]

*Zur fünften Frage*

**75** Mit seiner fünften Frage möchte das vorlegende Gericht im Wesentlichen wissen, ob Art. 82 Abs. 1 DSGVO dahin auszulegen ist, dass allein der Umstand, dass eine betroffene Person infolge eines Verstoßes gegen die DSGVO befürchtet, dass ihre personenbezogenen Daten durch Dritte missbräuchlich verwendet werden könnten, einen „immateriellen Schaden" im Sinne dieser Bestimmung darstellen kann.

**76** Was erstens den Wortlaut von Art. 82 Abs. 1 DSGVO betrifft, ist darauf hinzuweisen, dass dieser Folgendes vorsieht: „Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden

ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter."

**77** Insoweit hat der Gerichtshof festgestellt, dass aus dem Wortlaut von Art. 82 Abs. 1 DSGVO klar hervorgeht, dass das Vorliegen eines „Schadens", der entstanden ist, eine der Voraussetzungen für den in dieser Bestimmung vorgesehenen Schadenersatzanspruch darstellt, ebenso wie das Vorliegen eines Verstoßes gegen die DSGVO und eines Kausalzusammenhangs zwischen dem Schaden und dem Verstoß, wobei diese drei Voraussetzungen kumulativ sind (Urt. v. 4. 5. 2023, Österreichische Post [Immaterieller Schaden im Zusammenhang mit der Verarbeitung personenbezogener Daten], C-300/21, [K&R 2023, 416 ff. =] EU:C:2023:370, Rn. 32).

**78** Darüber hinaus hat der Gerichtshof Art. 82 Abs. 1 DSGVO auf der Grundlage von Erwägungen zu Wortlaut, Systematik sowie Sinn und Zweck dahin ausgelegt, dass er einer nationalen Regelung oder Praxis entgegensteht, die den Ersatz eines „immateriellen Schadens" im Sinne dieser Bestimmung davon abhängig macht, dass der der betroffenen Person entstandene Schaden einen bestimmten Grad an Erheblichkeit erreicht hat (Urt. v. 4. 5. 2023, Österreichische Post [Immaterieller Schaden im Zusammenhang mit der Verarbeitung personenbezogener Daten], C-300/21, [K&R 2023, 416 ff. =] EU:C:2023:370, Rn. 51).

**79** Weiter ist im vorliegenden Fall festzustellen, dass Art. 82 Abs. 1 DSGVO nicht danach unterscheidet, ob der infolge eines erwiesenen Verstoßes gegen die Bestimmungen der DSGVO von der betroffenen Person behauptete „immaterielle Schaden" mit einer zum Zeitpunkt ihres Schadenersatzantrags bereits erfolgten missbräuchlichen Verwendung ihrer personenbezogenen Daten durch Dritte verbunden ist oder ob er mit ihrer Angst verknüpft ist, dass eine solche Verwendung in Zukunft erfolgen könnte.

**80** Somit schließt der Wortlaut von Art. 82 Abs. 1 DSGVO nicht aus, dass der in dieser Bestimmung enthaltene Begriff „immaterieller Schaden" eine Situation wie die vom vorlegenden Gericht beschriebene umfasst, in der sich die betroffene Person, um Schadenersatz nach dieser Bestimmung zu erhalten, auf ihre Befürchtung beruft, dass ihre personenbezogenen Daten aufgrund des eingetretenen Verstoßes gegen die DSGVO in Zukunft von Dritten missbräuchlich verwendet werden.

**81** Diese wörtliche Auslegung wird zweitens durch den 146. Erwägungsgrund der DSGVO bestätigt, der speziell den in Art. 82 Abs. 1 DSGVO vorgesehenen Schadenersatzanspruch betrifft und in dessen drittem Satz es heißt, dass „[d]er Begriff des Schadens … im Lichte der Rechtsprechung des Gerichtshofs weit auf eine Art und Weise ausgelegt werden [sollte], die den Zielen dieser Verordnung in vollem Umfang entspricht." Eine Auslegung des Begriffs „immaterieller Schaden" im Sinne von Art. 82 Abs. 1 DSGVO, die nicht die Fälle umfasst, in denen die von einem Verstoß gegen die DSGVO betroffene Person sich auf die Befürchtung beruft, dass ihre eigenen personenbezogenen Daten in Zukunft missbräuchlich verwendet werden, entspräche jedoch nicht einer weiten Auslegung dieses Begriffs, wie sie vom Unionsgesetzgeber beabsichtigt ist (vgl. entsprechend Urt. v. 4. 5. 2023, Österreichische Post [Immaterieller Schaden im Zusammenhang mit der Verarbeitung personenbezogener Daten], C-300/21, [K&R 2023, 416 ff. =] EU:C:2023:370, Rn. 37 und 46).

**82** Zudem heißt es im ersten Satz des 85. Erwägungsgrundes der DSGVO, dass „[e]ine Verletzung des Schutzes personenbezogener Daten … – wenn nicht rechtzeitig und angemessen reagiert wird – einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen [kann], wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste … oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person". Aus dieser beispielhaften Aufzählung der „Schäden", die den betroffenen Personen entstehen können, geht hervor, dass der Unionsgesetzgeber unter den Begriff „Schaden" insbesondere auch den bloßen „Verlust der Kontrolle" über ihre eigenen Daten infolge eines Verstoßes gegen die DSGVO fassen wollte, selbst wenn konkret keine missbräuchliche Verwendung der betreffenden Daten zum Nachteil dieser Personen erfolgt sein sollte.

**83** Drittens und letztens wird die in Rn. 80 des vorliegenden Urteils vorgenommene Auslegung durch die Ziele der DSGVO gestützt, denen die Definition des Begriffs „Schaden" in vollem Umfang entsprechen muss, wie es im dritten Satz des 146. Erwägungsgrundes der DSGVO heißt. Eine Auslegung von Art. 82 Abs. 1 DSGVO dahin, dass der Begriff „immaterieller Schaden" im Sinne dieser Bestimmung keine Situationen umfasst, in denen sich eine betroffene Person nur auf ihre Befürchtung beruft, dass ihre Daten in Zukunft von Dritten missbräuchlich verwendet werden, wäre jedoch nicht mit der Gewährleistung eines hohen Schutzniveaus für natürliche Personen bei der Verarbeitung personenbezogener Daten in der Union vereinbar, die mit diesem Rechtsakt bezweckt wird.

**84** Allerdings ist darauf hinzuweisen, dass eine Person, die von einem Verstoß gegen die DSGVO betroffen ist, der für sie negative Folgen gehabt hat, nachweisen muss, dass diese Folgen einen immateriellen Schaden im Sinne von Art. 82 DSGVO darstellen (vgl. in diesem Sinne Urt. v. 4. 5. 2023, Österreichische Post [Immaterieller Schaden im Zusammenhang mit der Verarbeitung personenbezogener Daten], C-300/21, [K&R 2023, 416 ff. =] EU:C:2023:370, Rn. 50).

**85** Insbesondere muss das angerufene nationale Gericht, wenn sich eine Person, die auf dieser Grundlage Schadenersatz fordert, auf die Befürchtung beruft, dass ihre personenbezogenen Daten in Zukunft aufgrund eines solchen Verstoßes missbräuchlich verwendet werden, prüfen, ob diese Befürchtung unter den gegebenen besonderen Umständen und im Hinblick auf die betroffene Person als begründet angesehen werden kann.

**86** Nach alledem ist auf die fünfte Frage [wie im Tenor, Punkt 6] zu antworten […]

RA Peter Hense*

# Kommentar

Das Urteil der 3. Kammer des Gerichtshofs unter dem Vorsitz der Kammerpäsidentin der 3. Kammer *Jürimäe* sowie dem Berichterstatter *Jääskinen* wurde im April 2023 von den Schlussanträgen des Generalanwalts *Pitruzella* eingeleitet. Diese Anträge waren bereits anders betroffenenfreundlicher akzentuiert als die des Generalanwalts *Campos Sánchez-Bordona* in der Rechtssache C-300/21 – Österreichische Post, welche ebenfalls bei der 3. Kammer anhängig war. Fragen zum Schadensersatzrecht bilden den derzeit umfangreichsten Komplex zu entscheidender Rechtsfragen zur Anwendung der DSGVO mit über einem Dutzend anhängiger Vorlagefragen.

* Mehr über den Autor erfahren Sie am Ende des Kommentars.

Der Sachverhalt der Entscheidung steht pars pro toto für eine Vielzahl von ähnlichen Schadensersatzverfahren, die derzeit in der Europäischen Union vor nationalen Gerichten anhängig sind, und ist daher von erheblicher Praxisrelevanz: Ein Verantwortlicher, hier die staatliche Steuerbehörde, erleidet durch einen Angriff Dritter ein Datenleck, die personenbezogenen Daten von Betroffenen fließen ab und sind auf Dauer der Kontrolle der Berechtigten entzogen. Eine Betroffene forderte nunmehr Schadensersatz für eine auch ihr gegenüber erfolgte Datenschutzrechtsverletzung, wobei sie sich darauf beruft, dass die Behörde grundlegende Anforderungen der Informationssicherheit aus Art. 24 und 32 nicht beachtet, damit zur Entstehung des Schadens beigetragen und nun für den entstandenen Schaden einzustehen hat. Die Bestimmung von Art und Qualität des Schadens nach einem Datenkontrollverlust des Verantwortlichen ist Gegenstand einer nicht mehr zu überblickenden Vielzahl von Publikationen allein in Deutschland,[1] wobei der Fokus stark auf dem Begriff des „immateriellen" Schadens liegt, obwohl das Begriffspaar „materiell und immateriell" in Art. 82 nur klarstellend in Bezug auf jahrzehntelange Diskussionen um die vom Wortlaut knapp geratene Vorgängervorschrift Art. 23 Abs. 1 der Datenschutzrichtlinie 95/46/EG aufgenommen wurde, aber keine eigenständige Bedeutung aufweist. Im europäischen Datenschutzrecht ist ein Schaden ein Schaden, ganz egal, wie und wo die Schadenspositionen entstanden sind oder entstehen werden. Das ergibt auch Sinn, denn die Abgrenzung von materiellem und immateriellem Schadensersatz erfolgt bereits in den nationalen Rechtsordnungen nicht immer konturenscharf und unterliegt ständigem Wandel.

## I. Kein Automatismus: Ein „Datenleck" impliziert nicht automatisch unzureichende Datensicherheit

Lehrreicher als das Urteil selbst sind die Ausführungen des Generalanwalts ab Rn. 15 der Schlussanträge, nicht zuletzt aufgrund der aufschlussreichen Kommentare und Fußnoten. Der Gerichtshof schließt sich im Urteil diesen Ausführungen im Wesentlichen an und verdeutlicht neben dem Erfordernis unionsrechtsautonomer Auslegung (Rn. 23 des Urteils) die aufeinander abgestimmte, mehrstufige Systematik von Art. 24 und 32 und deren Zusammenspiel mit der alles umfassenden Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO.

Art. 24 DSGVO legt fest, dass es in der Verantwortung des Datenverarbeiters liegt, sowohl technische als auch organisatorische Maßnahmen zu ergreifen. Das Ziel dieser Maßnahmen ist es, die Einhaltung der Verordnung nicht nur zu sichern, sondern auch nachweislich zu belegen. Art. 32 der DSGVO konkretisiert diese Pflicht, indem er einen speziellen Schwerpunkt auf die Sicherheit der Datenverarbeitung legt. Zusammen präzisieren die Art. 24 und 32 die Anforderungen, die bereits in Art. 5 Abs. 2 umrissen sind. Hier wird unter den „Grundsätzen für die Verarbeitung personenbezogener Daten" der Grundsatz der „Rechenschaftspflicht" eingeführt. Dieser ergibt sich logisch aus dem in Art. 5 Abs. 1 lit. f verankerten Prinzip der „Integrität und Vertraulichkeit" und ergänzt diese. Beide Grundsätze sollten im Kontext des risikobasierten Ansatzes interpretiert werden, der zumindest an dieser Stelle unbestritten im Normtext der DSGVO Ausdruck findet.

Der Gerichtshof unterstreicht diese Aussagen durch Verweis darauf, dass Art. 24 Abs. 1 und 3 sowie Art. 32 Abs. 3 die allgemeine Rechenschaftspflicht des Verantwortlichen aus Art. 5 Abs. 2 präzisieren (Rn. 34 des Urteils).

In Rn. 26 der Schlussanträge klärt der Generalanwalt auf, was sich seiner Ansicht nach hinter dem Begriff „geeignet" in Art. 24 verbirgt. Der unbestimmte Rechtsbegriff „geeignet" setze voraus, dass die zur Absicherung von Informationssystemen ergriffenen Maßnahmen ein angemessenes Niveau sowohl in technischer (abstrakte Angemessenheit der Maßnahmen) als auch in qualitativer (konkrete Wirksamkeit des Schutzes) Hinsicht erreichen müssen. Für die Gewährleistung der Einhaltung der Prinzipien der Notwendigkeit, Angemessenheit und Verhältnismäßigkeit ist erforderlich, dass die konkrete Verarbeitung nicht nur zweckmäßig, sondern auch zielgerichtet erfolgt. Hierbei ist der Grundsatz der Datenminimierung von zentraler Bedeutung, welcher fordert, dass zu jedem Zeitpunkt der Datenverarbeitung stets eine Minimierung von Sicherheitsrisiken angestrebt wird.

Wenn der Generalanwalt feststellt, dass Art. 32 die Anforderungen an die technischen und organisatorischen Maßnahmen um Aspekte wie den Stand der Technik und die Implementierungskosten erweitert und damit nicht nur auf abstrakte Wirksamkeit, sondern auch Praktikabilität und wirtschaftliche Vertretbarkeit zu berücksichtigen sind, so schließt sich der Gerichtshof diesen Ausführungen in Rn. 26 des Urteils an und analysiert Art. 32 Absatz für Absatz (Rn. 26 - 28), um schließlich festzustellen, dass das gesetzliche Risikomanagement der DSGVO nicht auf Risikobeseitigung ausgelegt ist, sondern auf Risikominimierung (Rn. 29 des Urteils). Das Urteil rekurriert in Rn. 35 bis 38 schließlich auf die Erwägungsgründe 74, 76 und 83, aus deren Wortlaut und Systematik sich jeweils ergibt, dass ein „Eindämmen" von Risiken, nicht jedoch eine „Beseitigung" das legitime gesetzgeberische Ziel war.

## II. DSGVO erfordert effektives Compliance-Management, keine formale Checklistensicherheit

Der Generalanwalt betont, dass es weniger um die formale Einhaltung einzelner Vorschriften geht, sondern vielmehr um eine ganzheitliche Datenschutzstrategie des Unternehmens. Diese Gesamtstrategie ist entscheidend für die Befreiung von der Haftung. Dieser Ansatz spiegelt den risikobasierten und verantwortungsorientierten Ansatz der DSGVO wider, der von Unternehmen verlangt, dass sie Datenschutz als integralen Bestandteil ihrer Geschäftsprozesse verstehen und nicht nur als eine Reihe von Vorschriften, die es zu befolgen gilt.

Lesenswert ist der Hinweis des Generalanwalts in Fußnote 8 der Schlussanträge, worin er auf den ausgezeichneten Kommentar von *Kuner, Bygrave, Docksey* und *Drechsler*[2] verweist, die ihrerseits feststellen, dass die Prinzipien und Verpflichtungen der Datenschutzbestimmungen tief in das kulturelle Gefüge von Organisationen auf allen Ebenen eingebettet sein sollten, anstatt als eine Reihe von rechtlichen Anforderungen angesehen zu werden, die lediglich von der Rechtsabteilung abzuhaken sind.

Die Ausführungen des Generalanwalts in Rn. 43 der Anträge lesen sich vor diesem Hintergrund wie ein mahnender Eintrag ins Poesiealbum der Compliance-Abteilungen von Verantwortlichen, deren Aufgabe es ist, auch präventiv wirksam zu agieren und einen effektiven Plan-Do-Check-Act-Zyklus zu etablieren.[3]

1 Grundlegend: *Ettig/Herbrich*, K&R 2021, Beilage 1 zu Heft 6, 27 ff.
2 *Kuner/Bygrave/Docksey/Drechsler*, The EU General Data Protection Regulation (GDPR) A Commentary, 2018.
3 Vgl. auch die Etablierung dieser unionsrechtlichen Compliance-Pflicht durch den EuGH in C-129/21, K&R 2022, 826 ff., Rn. 67 – Proximus, dazu Besprechung *Hense*, ZD 2023, 212, 214.

## III. Richterliche Unabhängigkeit und Sorgfalt unerlässlich für effektiven Rechtsschutz

In seinen Ausführungen zur zweiten Vorlagefrage nimmt der EuGH die nationalen Gerichte in die Pflicht und fordert eine konkrete richterliche Beurteilung der Eignung technischer und organisatorischer Maßnahmen im Lichte von Art. 32 DSGVO. Der Gerichtshof hebt hervor, dass eine umfassende, risikoorientierte Analyse, die über eine oberflächliche Betrachtung der vom Verantwortlichen verfolgten Datenschutzstrategie hinausgeht, unerlässlich ist. Besonderer Nachdruck wird auf den Entscheidungsspielraum des Verantwortlichen gelegt, der jedoch einer sorgfältigen und tiefgreifenden gerichtlichen Prüfung standhalten muss.

Diese Prüfung, die auf einer fundierten Beurteilung der Art, des Inhalts und der praktischen Umsetzung der Datenschutzmaßnahmen beruht, zielt darauf ab, ein angemessenes Sicherheitsniveau im Kontext der spezifischen Risiken der Datenverarbeitung zu gewährleisten. Das Urteil betont somit die Bedeutung der Effektivität des Datenschutzes und des Rechts auf einen wirksamen gerichtlichen Rechtsbehelf, indem es eine gründliche und individuelle Untersuchung der vom Verantwortlichen getroffenen Maßnahmen im Einklang mit den Anforderungen der DSGVO verlangt. Dadurch wird eine Brücke zwischen nur formaler, genereller Rechtskonformität und praktischer, konkreter Wirksamkeit des Datenschutzes geschlagen, was die zentrale Rolle der Gerichte in der Durchsetzung der Datenschutzvorschriften unterstreicht.

## IV. Rechenschaft und Verantwortlichkeit

In seiner Antwort auf den ersten Teil der dritten Vorlagefrage behandelt der EuGH erneut zentrale Aspekte der Rechenschaftspflicht und der Verantwortlichkeit. Der Gerichtshof befasst sich mit der Frage, ob der Verantwortliche im Kontext einer auf Art. 82 basierenden Schadensersatzklage die Beweislast dafür trägt, dass seine Sicherheitsmaßnahmen gemäß Art. 32 DSGVO geeignet waren. Art. 5 Abs. 2 und Art. 24 DSGVO etablieren den Grundsatz der Rechenschaftspflicht, wonach der Verantwortliche nicht nur für die Einhaltung der Datenschutzprinzipien verantwortlich ist, sondern auch beweisen muss, dass diese Prinzipien eingehalten werden (Rn. 52 des Urteils).

Das Urteil illustriert mit unmissverständlicher Klarheit, dass gemäß Art. 32 DSGVO der Verantwortliche verbindlich dazu angehalten ist, geeignete technische und organisatorische Maßnahmen zu implementieren. Ferner obliegt es dem Verantwortlichen nach Art. 24, 5 Abs. 2 DSGVO, zur Überzeugung des Gerichts zu belegen, dass diese Maßnahmen eine Datenverarbeitung garantieren, die in vollständiger Übereinstimmung mit den Anforderungen der DSGVO steht. Diese Beweislastverteilung ist gerechtfertigt, denn es ist der ideal informierte Verantwortliche, der umfassendes Wissen über seine Systeme, Verarbeitungsvorgänge und die damit verbundenen Risiken besitzt, der die Wirksamkeit seiner Maßnahmen nachzuweisen hat. Die mitunter postulierte Erwartung, wonach Betroffene, die keinen Zugang zu diesem spezifischen Wissen haben, beweisen müssten, dass die vom Verantwortlichen getroffenen Maßnahmen unzureichend waren, geht an der Lebensrealität völlig vorbei. Der Einsatz von IT-Systemen bringt für die Verantwortlichen Vorteile mit sich, woraus sich zugleich die Verpflichtung ergibt, den vollumfänglichen Nachweis ihrer rechtskonformen Anwendung zu erbringen. Dieser Grundsatz lässt sich treffend mit dem lateinischen Sprichwort „Cuius est commodum, eius est periculum“ umschreiben. Es bedeutet, dass derjenige, der den Nutzen aus einer Sache zieht, auch die damit verbundenen Risiken und Verantwortlichkeiten tragen muss.[4]

Der Gerichtshof betont, dass eine solche Auslegung die Ziele der DSGVO stützt, insbesondere die Stärkung der Rechte betroffener Personen und die Verschärfung der Verantwortlichkeiten der Datenverarbeiter. Würde die Beweislast auf die betroffenen Personen gelegt, nähme dies dem Schadenersatzanspruch nach Art. 82 Abs. 1 DSGVO seine praktische Wirksamkeit (Rn. 56 des Urteils).

## V. Kein Automatismus, wonach ein Gutachten eine gerichtliche Entscheidung präjudiziert

Der Gerichtshof konzentriert sich auf den zweiten Teil der dritten Frage des vorlegenden Gerichts, die die Notwendigkeit und Suffizienz eines solchen Gutachtens als Beweismittel in Schadensersatzklagen nach Art. 82 DSGVO betrifft. Der EuGH stellt klar, dass die DSGVO keine spezifischen Regeln über die Zulassung und den Beweiswert von Beweismitteln wie gerichtlichen Sachverständigengutachten vorgibt. Stattdessen unterliegt dies dem Grundsatz der Verfahrensautonomie der Mitgliedstaaten, solange die Äquivalenz- und Effektivitätsgrundsätze des Unionsrechts eingehalten werden (Rn. 60 des Urteils). Diese Grundsätze besagen, dass die nationalen Verfahrensregeln bei der Anwendung von Unionsrecht nicht ungünstiger als bei der Anwendung von nationalem Recht sein sowie die Ausübung von durch das Unionsrecht verliehenen Rechten nicht praktisch unmöglich machen oder übermäßig erschweren dürfen. Das Gericht betont, dass eine generelle Vorschrift, die Sachverständigengutachten als notwendig erachtet, gegen den Effektivitätsgrundsatz verstoßen könnte, insbesondere wenn andere Beweismittel verfügbar sind, wie etwa Ergebnisse einer kürzlich durchgeführten Kontrolle der Datenschutzmaßnahmen durch eine unabhängige Behörde (Rn. 62 des Urteils). Ebenso könnte eine Regelung, die ein Sachverständigengutachten als ausreichendes Beweismittel betrachtet, den Effektivitätsgrundsatz verletzen, da sie die objektive Beurteilung der Geeignetheit der Maßnahmen durch ein unparteiisches Gericht untergraben würde. Erneut hebt der EuGH den Wert des in Art. 79 Abs. 1 DSGVO garantierten Rechts auf wirksamen gerichtlichen Rechtsbehelf hervor, für dessen Effektivität sich oberflächliche Automatismen verbieten und der vielmehr eine originäre, umfassende und tiefgehende gerichtliche Beweiswürdigung erfordert (Rn. 63 des Urteils). Dieser Appell des Gerichtshofs sollte auch von deutschen Gerichten Beachtung finden, insbesondere von jenen, deren Aufgabe es ist, spezialisierte Spruchkörper zu etablieren. Die Instanzen sind dazu berufen, Recht zu sprechen und fundierte Entscheidungen zu treffen, anstatt wie oft im Datenschutzrecht ungerichtet im Nebel zu agieren.

## VI. Kein Automatismus, wonach der Verantwortliche durch Eingreifen „Dritter“ automatisch von seiner Haftung befreit würde

Art. 82 Abs. 2 etabliert die Haftung jedes Verantwortlichen für Schäden, die aus nicht DSGVO-konformer Verarbeitung entstehen. Art. 82 Abs. 3 DSGVO präzisiert, dass der Verantwortliche von der Haftung befreit wird, wenn er nachweisen kann, dass er in keinerlei Hinsicht für den schadensverursachenden Umstand verantwortlich ist. Der Gerichtshof betont, dass diese Befreiung von der Haftung strengen Bedingungen unterliegt

4 Dazu *Hense*, ZD 2022, 413 ff.

und nur dann greift, wenn der Verantwortliche keinen Anteil an der Verursachung des Schadens hat.

Bei Datenschutzverletzungen durch Cyberkriminelle muss der Verantwortliche nachweisen, dass kein Kausalzusammenhang zwischen seiner möglichen Verletzung der Datenschutzpflichten und dem entstandenen Schaden besteht. Dies bedeutet, dass der Verantwortliche nicht automatisch von der Haftung befreit wird, nur weil der Schaden durch Dritte verursacht wurde. Vielmehr muss er belegen, dass er alle erforderlichen und angemessenen Maßnahmen gemäß der DSGVO ergriffen hat, um die Verletzung zu verhindern.

### VII. Furcht und Schaden

Die fünfte Frage des vorlegenden Gerichts betrifft die Interpretation von Art. 82 Abs. 1 in Bezug auf die Befürchtung einer betroffenen Person, dass ihre personenbezogenen Daten infolge eines Verstoßes gegen die DSGVO missbräuchlich verwendet werden könnten, und ob dies allein einen „immateriellen Schaden" im Sinne der Verordnung darstellen kann.

Die Kammer zählt zunächst ihre mittlerweile gefestigten Kriterien auf, dass für einen Schadenersatzanspruch nach Art. 82 Abs. 1 eine Trias vorliegen muss, nämlich (1) ein Schaden, (2) ein Verstoß gegen die DSGVO und (3) ein Kausalzusammenhang zwischen Schaden und Verstoß. Nicht mehr, nicht weniger.

Der Gerichtshof hebt unter Rückgriff auf das eigene Grundsatzurteil der Kammer in Sachen C-300/21[5] hervor, dass die DSGVO an keiner Stelle einen bestimmten Grad an Erheblichkeit für die Kompensationsfähigkeit eines (immateriellen) Schadens voraussetzt und dass der Begriff des Schadens selbst „weit" ausgelegt werden sollte. Denkbar einfache Kriterien, könnte man meinen. Der Gerichtshof nimmt dabei immer wieder auf ErwG 146 Bezug, der das Kriterium der „Weite" ausdrücklich postuliert. Auch wenn den Erwägungsgründen selbst keine rechtliche Bindungswirkung zukommt,[6] so spielen sie in der Rechtsprechung des EuGH eine gewichtige Rolle, denn sofern der Rahmen der Norm gewahrt und der Wortlaut der Norm nicht offensichtlich gegen den Strich gebürstet wird, entfalten Erwägungsgründe ihren bemerkenswert wirkmächtigen intellektuellen und kreativen Einfluss auf die Auslegung des Unionsrechts. Wenn also der ErwG 146 vom Rechtsanwender „Weite" bei der Auslegung des unionsrechtlichen Schadensbegriffs fordert, so schlussfolgert der Gerichtshof, dass dies die Befürchtung einer missbräuchlichen Verwendung personenbezogener Daten in der Zukunft miteinschließt. Denn auch der ErwG 85 erwähne ja, dass eine Verletzung des Datenschutzes immaterielle Schäden wie den Verlust der Kontrolle über persönliche Daten nach sich ziehen kann, selbst wenn keine konkrete missbräuchliche Verwendung der Daten stattgefunden hat. Dies deckt sich auch mit den Ausführungen in Rn. 22 einer weiteren aktuellen Entscheidung der 3. Kammer in Sachen „Gemeinde Ummendorf",[7] wo bereits die kurzzeitige Veröffentlichung personenbezogener Daten eines Betroffenen im Internet ohne das Hinzutreten weiterer schadensvertiefender Umstände als kompensationsfähiger Schaden unter dem Gesichtspunkt des Kontrollverlusts nach ErwG 146 angesehen wurde.

Der Gerichtshof betont im vorliegenden Fall, dass seine Auslegung von Art. 82 im Einklang mit den Zielen der DSGVO steht, die ein hohes Schutzniveau für natürliche Personen bei der Verarbeitung personenbezogener Daten anstreben. Eine Auslegung, die die Befürchtung einer missbräuchlichen Verwendung von Daten nicht als immateriellen Schaden anerkennt, wäre nicht mit diesem Ziel vereinbar.

Das Gericht grenzt jedoch ein: Betroffene müssen nachweisen, dass die von ihnen vorgetragenen negativen Folgen einen Schaden darstellen, und das nationale Gericht muss prüfen, ob die Befürchtung der betroffenen Person unter den gegebenen Umständen als begründet angesehen werden können (Rn. 84 f. des Urteils). Ob sich aus diesen eher prozessualen Erwägungen tatsächliche materiellrechtliche Einschränkungen ergeben können, ist zu bezweifeln. Es liegt auf der Hand zu fragen, wie die nationalen Gerichte prüfen sollen, ob eine „Befürchtung" begründet war. Auch hier gibt die 3. Kammer Leitlinien auf den Weg,[8] indem der Gerichtshof formuliert, dass über die genannte Trias von Schaden, Verstoß und Kausalität hinaus für die Haftung nach Art. 82 Abs. 1 keine weiteren Voraussetzungen aufgestellt werden dürfen, etwa die, dass der Nachteil spürbar oder die Beeinträchtigung objektiv sein muss. Begründet muss die Furcht als Schaden also sein, aber nicht objektivierbar oder spürbar, denn beiden Kriterien wohnen Anklänge an eine nunmehr in ständiger Rechtsprechung entschieden abgelehnte Bagatellgrenze inne.

**Peter Hense**

ist Rechtsanwalt und Gründungspartner bei Spirit Legal LLP. Er ist Experte für Technologierecht und berät zu internationalem IT- und Technologierecht, dem Recht der Nutzung von Daten sowie in der Prozessführung (Privacy Litigation), insbesondere im Bereich Advertising Technology, Machine Learning sowie zur Ethik automatisierter Entscheidungssysteme (Accountable AI).

5 EuGH, 4. 5. 2023 – C-300/21, K&R 2023, 416 ff., Rn. 32 – Österreichische Post
6 EuGH, 19. 6. 2014 – C-345/13, Rn. 31 – Karen Millen Fashions.
7 EuGH, 14. 10. 2023 – C-456/22, K&R 2024, 112 ff. (in diesem Heft).
8 EuGH, 14. 10. 2023 – C-456/22, K&R 2024, 112 ff., Rn. 17 (in diesem Heft).

## Nachweispflicht bei Schadensersatz wegen Datenschutzverstoß

**EuGH**, Urteil vom 14. 12. 2023 – C-456/22

**Volltext-ID**: KuRL2024-112, www.kommunikationundrecht.de

VX, AT ./. Gemeinde Ummendorf

ECLI:EU:C:2023:988

Verfahrensgang: LG Ravensburg, 30. 6. 2022

Art. 82 Abs. 1 VO (EU) 2016/679

**Art. 82 Abs. 1 der VO (EU) 2016/679 […] ist dahin auszulegen, dass er einer nationalen Rechtsvorschrift oder -praxis entgegensteht, die für einen durch einen Verstoß gegen diese Verordnung verursachten immateriellen Schaden eine „Bagatellgrenze" vorsieht. Die betroffene Person muss den Nachweis erbringen, dass die Folgen dieses Verstoßes, die sie erlitten zu haben behauptet, ursächlich für einen Schaden waren, der sich von der bloßen Verletzung der Bestimmungen dieser Verordnung unterscheidet. (Tenor des Gerichts)**

#### Sachverhalt

Das Vorabentscheidungsersuchen betrifft die Auslegung von Art. 82 Abs. 1 der VO (EU) 2016/679 des Europäischen Par-