Vorläufige Fassung

URTEIL DES GERICHTSHOFS (Dritte Kammer)

14. Dezember 2023(*)

„Vorlage zur Vorabentscheidung – Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten – Verordnung (EU) 2016/679 – Art. 5 – Grundsätze dieser Verarbeitung – Art. 24 – Verantwortung des für die Verarbeitung Verantwortlichen – Art. 32 – Zur Gewährleistung der Sicherheit der Verarbeitung getroffene Maßnahmen – Beurteilung der Geeignetheit solcher Maßnahmen – Umfang der gerichtlichen Überprüfung – Beweisführung – Art. 82 – Haftung und Recht auf Schadenersatz – Mögliche Befreiung des Verantwortlichen von der Haftung bei Verstößen durch Dritte – Klage auf Ersatz eines immateriellen Schadens aufgrund der Befürchtung eines möglichen Missbrauchs personenbezogener Daten“

In der Rechtssache C-340/21

betreffend ein Vorabentscheidungsersuchen nach Art. 267 AEUV, eingereicht vom Varhoven administrativen sad (Oberstes Verwaltungsgericht, Bulgarien) mit Entscheidung vom 14. Mai 2021, beim Gerichtshof eingegangen am 2. Juni 2021, in dem Verfahren

VB

gegen

Natsionalna agentsia za prihodite

erlässt

DER GERICHTSHOF (Dritte Kammer)

unter Mitwirkung der Kammerpräsidentin K. Jürimäe sowie der Richter N. Piçarra, M. Safjan, N. Jääskinen (Berichterstatter) und M. Gavalec,

Generalanwalt: G. Pitruzzella,

Kanzler: A. Calot Escobar,

aufgrund des schriftlichen Verfahrens,

unter Berücksichtigung der Erklärungen

– der Natsionalna agentsia za prihodite, vertreten durch R. Spetsov,

– der bulgarischen Regierung, vertreten durch M. Georgieva und L. Zaharieva als Bevollmächtigte,

– der tschechischen Regierung, vertreten durch O. Serdula, M. Smolek und J. Vláčil als Bevollmächtigte,

– von Irland, vertreten durch M. Browne, Chief State Solicitor, A. Joyce, J. Quaney und M. Tierney als Bevollmächtigte im Beistand von D. Fennelly, BL,

– der italienischen Regierung, vertreten durch G. Palmieri als Bevollmächtigte im Beistand von

E. De Bonis, Avvocato dello Stato,

– der portugiesischen Regierung, vertreten durch P. Barros da Costa, A. Pimenta, M. J. Ramos und C. Vieira Guerra als Bevollmächtigte,

– der Europäischen Kommission, vertreten durch A. Bouchagiar, H. Kranenborg und N. Nikolova als Bevollmächtigte,

nach Anhörung der Schlussanträge des Generalanwalts in der Sitzung vom 27. April 2023

folgendes

Urteil

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

2 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.

Rechtlicher Rahmen

3 In den Erwägungsgründen 4, 10, 11, 74, 76, 83, 85 und 146 der DSGVO heißt es:

„(4) … Diese Verordnung steht im Einklang mit allen Grundrechten und achtet alle Freiheiten und Grundsätze, die mit der [Charta der Grundrechte der Europäischen Union] anerkannt wurden und in den Europäischen Verträgen verankert sind, insbesondere Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation, Schutz personenbezogener Daten, … Recht auf einen wirksamen Rechtsbehelf und ein faires Verfahren …

…

(10) Um ein gleichmäßiges und hohes Datenschutzniveau für natürliche Personen zu gewährleisten und die Hemmnisse für den Verkehr personenbezogener Daten in der [Europäischen] Union zu beseitigen, sollte das Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung dieser Daten in allen Mitgliedstaaten gleichwertig sein. Die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten von natürlichen Personen bei der Verarbeitung personenbezogener Daten sollten unionsweit gleichmäßig und einheitlich angewandt werden. …

(11) Ein unionsweiter wirksamer Schutz personenbezogener Daten erfordert die Stärkung und präzise Festlegung der Rechte der betroffenen Personen sowie eine Verschärfung der Verpflichtungen für diejenigen, die personenbezogene Daten verarbeiten und darüber entscheiden, …

…

(74) Die Verantwortung und Haftung des Verantwortlichen für jedwede Verarbeitung

personenbezogener Daten, die durch ihn oder in seinem Namen erfolgt, sollte geregelt werden. Insbesondere sollte der Verantwortliche geeignete und wirksame Maßnahmen treffen müssen und nachweisen können, dass die Verarbeitungstätigkeiten im Einklang mit dieser Verordnung stehen und die Maßnahmen auch wirksam sind. Dabei sollte er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung und das Risiko für die Rechte und Freiheiten natürlicher Personen berücksichtigen.

…

(76) Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person sollten in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden. Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt.

…

(83) 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, wie etwa eine Verschlüsselung, treffen. Diese Maßnahmen sollten unter Berücksichtigung des Stands der Technik und der Implementierungskosten ein Schutzniveau – auch hinsichtlich der Vertraulichkeit – gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist. Bei der Bewertung der Datensicherheitsrisiken sollten die mit der Verarbeitung personenbezogener Daten verbundenen Risiken berücksichtigt werden, wie etwa – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von oder unbefugter Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, insbesondere wenn dies zu einem physischen, materiellen oder immateriellen Schaden führen könnte.

…

(85) Eine Verletzung des Schutzes personenbezogener Daten kann – wenn nicht rechtzeitig und angemessen reagiert wird – einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person. Deshalb sollte der Verantwortliche, sobald ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird, die Aufsichtsbehörde von der Verletzung des Schutzes personenbezogener Daten unverzüglich … unterrichten, …

…

(146) Der Verantwortliche oder der Auftragsverarbeiter sollte Schäden, die einer Person aufgrund einer Verarbeitung entstehen, die mit dieser Verordnung nicht im Einklang steht, ersetzen. Der Verantwortliche oder der Auftragsverarbeiter sollte von seiner Haftung befreit werden, wenn er nachweist, dass er in keiner Weise für den Schaden verantwortlich ist. Der Begriff des Schadens sollte im Lichte der Rechtsprechung des Gerichtshofs weit auf eine Art und Weise ausgelegt werden, die den Zielen dieser Verordnung in vollem Umfang entspricht. Dies gilt unbeschadet von Schadenersatzforderungen aufgrund von Verstößen gegen andere Vorschriften des Unionsrechts oder des Rechts der Mitgliedstaaten. Zu einer Verarbeitung, die mit der vorliegenden Verordnung nicht im Einklang steht, zählt auch eine Verarbeitung, die nicht mit den nach Maßgabe der vorliegenden Verordnung erlassenen delegierten Rechtsakten

und Durchführungsrechtsakten und Rechtsvorschriften der Mitgliedstaaten zur Präzisierung von Bestimmungen der vorliegenden Verordnung im Einklang steht. Die betroffenen Personen sollten einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhalten. …“

4 Art. 4 („Begriffsbestimmungen“) dieser Verordnung bestimmt:

„Im Sinne dieser Verordnung bezeichnet der Ausdruck:

1. ‚personenbezogene Daten‘ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden ‚betroffene Person‘) beziehen; …

2. ‚Verarbeitung‘ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten …;

…

7. ‚Verantwortlicher‘ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; …

…

10. ‚Dritter‘ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;

…

12. ‚Verletzung des Schutzes personenbezogener Daten‘ eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

…“

5 Art. 5 („Grundsätze für die Verarbeitung personenbezogener Daten“) DSGVO sieht vor:

„(1) Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (‚Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz‘);

…

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen (‚Integrität und Vertraulichkeit‘);

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können (‚Rechenschaftspflicht‘).“

6 Art. 24 („Verantwortung des für die Verarbeitung Verantwortlichen“) DSGVO lautet:

„(1) Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

(2) Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maßnahmen gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen durch den Verantwortlichen umfassen.

(3) Die Einhaltung der genehmigten Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.“

7 Art. 32 („Sicherheit der Verarbeitung“) DSGVO bestimmt:

„(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

(3) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

…“

8 Art. 79 („Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter“) Abs. 1 DSGVO bestimmt:

„Jede betroffene Person hat unbeschadet eines verfügbaren verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde gemäß Artikel 77 das Recht auf einen wirksamen gerichtlichen Rechtsbehelf, wenn sie der Ansicht ist, dass die ihr aufgrund dieser Verordnung zustehenden Rechte infolge einer nicht im Einklang mit dieser Verordnung stehenden Verarbeitung ihrer personenbezogenen Daten

verletzt wurden.“

9 Art. 82 („Haftung und Recht auf Schadenersatz“) Abs. 1 bis 3 DSGVO sieht vor:

„(1) 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.

(2) Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. …

(3) Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Absatz 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.“

Ausgangsrechtsstreit und Vorlagefragen

10 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.

11 Am 15. Juli 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.

12 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.

13 Vor diesem Hintergrund erhob die Klägerin des Ausgangsverfahrens beim Administrativen sad Sofia-grad (Verwaltungsgericht der Stadt Sofia, Bulgarien) auf der Grundlage von Art. 82 DSGVO und Bestimmungen des bulgarischen Rechts Klage auf Verurteilung der NAP zur Zahlung von 1 000 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 Buchst. 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.

14 Die NAP verteidigte sich damit, dass die Klägerin des Ausgangsverfahrens von ihr keine Informationen über die spezifischen Daten, die offengelegt worden seien, angefordert habe. Sie legte ferner Dokumente zum Nachweis dafür vor, dass sie alle erforderlichen Maßnahmen ergriffen habe, um im Vorfeld die Verletzung des Schutzes der in ihrem IT-System enthaltenen personenbezogenen Daten zu verhindern und im Nachhinein die Auswirkungen dieser Verletzung zu begrenzen und die Bürger zu beruhigen. Außerdem bestehe zwischen dem behaupteten immateriellen Schaden und der genannten Verletzung kein Kausalzusammenhang. Überdies könne sie nicht für die schädlichen Folgen dieser Verletzung verantwortlich gemacht werden, da sie selbst durch Personen, die nicht ihre Bediensteten seien, böswillig geschädigt worden sei.

15 Mit Entscheidung vom 27. November 2020 wies der Administrativen sad Sofia-grad (Verwaltungsgericht der Stadt Sofia) die Klage der Klägerin des Ausgangsverfahrens ab. Dieses

Gericht stellte zum einen fest, dass der unbefugte Zugriff auf die Datenbank der NAP auf einen von Dritten begangenen Hackerangriff zurückzuführen sei, und zum anderen, dass die Klägerin des Ausgangsverfahrens nicht nachgewiesen habe, dass die NAP es unterlassen habe, Sicherheitsmaßnahmen zu ergreifen. Zudem sei der Klägerin des Ausgangsverfahrens kein immaterieller Schaden entstanden, der einen Schadenersatzanspruch begründe.

16 Die Klägerin des Ausgangsverfahrens legte gegen diese Entscheidung Kassationsbeschwerde beim Varhoven administrativen sad (Oberstes Verwaltungsgericht, Bulgarien), dem vorlegenden Gericht in der vorliegenden Rechtssache, ein. Sie stützt ihr Rechtsmittel darauf, dass das erstinstanzliche Gericht bei der Verteilung der Beweislast hinsichtlich der von der NAP ergriffenen Sicherheitsmaßnahmen einen Rechtsfehler begangen habe, und dass die NAP nicht nachgewiesen habe, dass sie insoweit nicht untätig geblieben sei. Ferner sei die Befürchtung eines möglichen künftigen Missbrauchs ihrer personenbezogenen Daten ein tatsächlicher immaterieller und kein hypothetischer Schaden. Die NAP tritt allen diesen Argumenten entgegen.

17 Das vorlegende Gericht zieht zunächst die Möglichkeit in Betracht, dass schon die Feststellung einer Verletzung des Schutzes personenbezogener Daten den Schluss zulasse, dass die vom für die Verarbeitung dieser Daten Verantwortlichen getroffenen Maßnahmen nicht „geeignet“ im Sinne der Art. 24 und 32 DSGVO gewesen seien.

18 Für den Fall, dass diese Feststellung für die Bejahung einer solchen Schlussfolgerung nicht ausreichen sollte, fragt das vorlegende Gericht jedoch zum einen nach dem Umfang der Kontrolle, die die nationalen Gerichte bei der Beurteilung der Geeignetheit der betreffenden Maßnahmen vorzunehmen hätten, und zum anderen nach den Regeln der Beweisführung, die in diesem Rahmen sowohl in Bezug auf die Beweislast als auch in Bezug auf die Beweismittel anzuwenden seien, insbesondere, wenn diese Gerichte mit einer auf Art. 82 DSGVO gestützten Schadenersatzklage befasst seien.

19 Sodann möchte das vorlegende Gericht wissen, ob im Hinblick auf Art. 82 Abs. 3 DSGVO der Umstand, dass die Verletzung des Schutzes personenbezogener Daten auf eine von Dritten begangene Handlung, im vorliegenden Fall auf einen Cyberangriff, zurückzuführen sei, ein Kriterium sei, das den für die Verarbeitung dieser Daten Verantwortlichen generell von seiner Haftung für den der betroffenen Person entstandenen Schaden befreie.

20 Schließlich fragt sich das vorlegende Gericht, ob allein die Befürchtung einer Person, dass ihre personenbezogenen Daten, im vorliegenden Fall nach einem unbefugten Zugang zu ihnen und ihrer Offenlegung durch Cyberkriminelle, in Zukunft missbräuchlich verwendet werden könnten, einen „immateriellen Schaden“ im Sinne von Art. 82 Abs. 1 DSGVO darstellen könne. Sollte dies der Fall sein, müsste diese Person nicht nachweisen, dass Dritte diese Daten vor Erhebung ihrer Schadenersatzklage unrechtmäßig verwendet hätten, etwa durch Identitätsdiebstahl.

21 Unter diesen Umständen hat der Varhoven administrativen sad (Oberstes Verwaltungsgericht) das Verfahren ausgesetzt und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorgelegt:

1. Sind die Art. 24 und 32 DSGVO dahin auszulegen, dass es ausreicht, wenn eine unbefugte Offenlegung von beziehungsweise ein unbefugter Zugang zu personenbezogenen Daten im Sinne von Art. 4 Nr. 12 DSGVO durch Personen erfolgt ist, die keine Bediensteten der Verwaltung des Verantwortlichen sind und nicht seiner Kontrolle unterliegen, um anzunehmen, dass die getroffenen technischen und organisatorischen Maßnahmen nicht geeignet sind?

2. Falls die erste Frage verneint wird, welchen Gegenstand und Umfang sollte die gerichtliche Rechtmäßigkeitskontrolle bei der Prüfung haben, ob die vom Verantwortlichen getroffenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO geeignet sind?

3. Falls die erste Frage verneint wird, sind der Grundsatz der Rechenschaftspflicht nach Art. 5

Abs. 2 und Art. 24 in Verbindung mit dem 74. Erwägungsgrund der DSGVO dahin auszulegen, dass im Klageverfahren nach Art. 82 Abs. 1 DSGVO der Verantwortliche die Beweislast dafür trägt, dass die getroffenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO geeignet sind?

Kann die Einholung eines Sachverständigengutachtens als ein notwendiges und ausreichendes Beweismittel angesehen werden, um festzustellen, ob die vom Verantwortlichen getroffenen technischen und organisatorischen Maßnahmen in einem Fall wie dem vorliegenden geeignet waren, wenn der unbefugte Zugang zu und die unbefugte Offenlegung von personenbezogenen Daten Folge eines „Hackerangriffs“ sind?

4. Ist Art. 82 Abs. 3 DSGVO dahin auszulegen, dass die unbefugte Offenlegung von oder der unbefugte Zugang zu personenbezogenen Daten im Sinne von Art. 4 Nr. 12 DSGVO wie vorliegend mittels eines „Hackerangriffs“ durch Personen, die keine Bediensteten der Verwaltung des Verantwortlichen sind und nicht seiner Kontrolle unterliegen, einen Umstand darstellt, für den der Verantwortliche in keinerlei Hinsicht verantwortlich ist und der zur Befreiung von der Haftung berechtigt?

5. Sind Art. 82 Abs. 1 und 2 in Verbindung mit den Erwägungsgründen 85 und 146 der DSGVO dahin auszulegen, dass in einem Fall wie dem vorliegenden Fall einer Verletzung des Schutzes personenbezogener Daten, die sich in dem unbefugten Zugang zu und der Verbreitung von personenbezogenen Daten mittels eines „Hackerangriffs“ äußert, allein die von der betroffenen Person erlittenen Sorgen, Befürchtungen und Ängste vor einem möglichen künftigen Missbrauch personenbezogener Daten unter den weit auszulegenden Begriff des immateriellen Schadens fallen und zum Schadenersatz berechtigen, wenn ein solcher Missbrauch nicht festgestellt wurde und/oder kein weiterer Schaden der betroffenen Person entstanden ist?

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. Januar 1984, Ekro, 327/82, EU:C:1984:11, Rn. 11, vom 1. Oktober 2019, Planet49, C-673/17, EU:C:2019:801, Rn. 47 und 48, sowie vom 4. Mai 2023, Österreichische Post [Immaterieller Schaden im Zusammenhang mit der Verarbeitung personenbezogener Daten], C-300/21, 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 Satz 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 zu antworten, dass 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 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 DSGVO waren.

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 in Verbindung mit 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 zu antworten, dass 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 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.

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 Buchst. 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 in Verbindung mit 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 Buchst. f und Art. 32 DSGVO gewährleistet, dem für die betreffende Verarbeitung Verantwortlichen obliegt (vgl. entsprechend Urteile vom 4. Mai 2023, Bundesrepublik Deutschland [Elektronisches Gerichtsfach], C-60/22, EU:C:2023:373, Rn. 52 und 53, und vom 4. Juli 2023, Meta Platforms u. a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, 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 zu antworten, dass 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.

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) (Urteil vom 4. Mai 2023, Österreichische Post [Immaterieller Schaden im Zusammenhang mit der Verarbeitung personenbezogener Daten], C-300/21, 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. Juni 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, Rn. 297, und vom 4. Mai 2023, Österreichische Post [Immaterieller Schaden im Zusammenhang mit der Verarbeitung personenbezogener Daten], C-300/21, 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 Urteil vom 12. Januar 2023, Nemzeti Adatvédelmi és Információszabadság Hatóság, C-132/21, EU:C:2023:2, Rn. 50).

64 Nach alledem ist auf den zweiten Teil der dritten Frage zu antworten, dass 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 kein generell notwendiges und ausreichendes Beweismittel sein kann.

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 Buchst. 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 zu antworten, dass 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 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 DSGVO ist, wobei der Verantwortliche dann nachweisen muss, dass er in keinerlei Hinsicht für den Umstand, durch den der betreffende Schaden eingetreten ist, verantwortlich ist.

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 (Urteil vom 4. Mai 2023, Österreichische Post [Immaterieller Schaden im Zusammenhang mit der Verarbeitung personenbezogener Daten], C-300/21, 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 (Urteil vom 4. Mai 2023, Österreichische Post [Immaterieller Schaden im Zusammenhang mit der Verarbeitung personenbezogener Daten], C-300/21, 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 Urteil vom 4. Mai 2023, Österreichische Post [Immaterieller Schaden im Zusammenhang mit der Verarbeitung personenbezogener Daten], C-300/21, 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 Urteil vom 4. Mai 2023, Österreichische Post [Immaterieller Schaden im Zusammenhang mit der Verarbeitung personenbezogener Daten], C-300/21, 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 zu antworten, dass 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.

Kosten

87 Für die Beteiligten des Ausgangsverfahrens ist das Verfahren Teil des beim vorlegenden Gericht anhängigen Verfahrens; die Kostenentscheidung ist daher Sache dieses Gerichts. Die Auslagen anderer Beteiligter für die Abgabe von Erklärungen vor dem Gerichtshof sind nicht erstattungsfähig.

Aus diesen Gründen hat der Gerichtshof (Dritte Kammer) für Recht erkannt:

1. **Die Art. 24 und 32 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)**

   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 Verordnung 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 Verordnung 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 Verordnung 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 Verordnung 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 Verordnung 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.

Unterschriften

---

* Verfahrenssprache: Bulgarisch.