Rechtssache C-340/21

Zusammenfassung des Vorabentscheidungsersuchens gemäß Art. 98 Abs. 1 der Verfahrensordnung des Gerichtshofs

Eingangsdatum:

2. Juni 2021

Vorlegendes Gericht:

Varhoven administrativen sad (Bulgarien)

Datum der Vorlageentscheidung:

14. Mai 2021

Kassationsbeschwerdeführerin:

VB

Kassationsbeschwerdegegnerin:

Natsionalna agentsia za prihodite (Nationale Agentur für Einnahmen)

Gegenstand des Ausgangsverfahrens

Rechtsmittel gegen ein Urteil, mit dem die Klage auf Ersatz des immateriellen Schadens als unbegründet abgewiesen wurde, der aufgrund des rechtswidrigen Unterlassens der Kassationsbeschwerdegegnerin in ihrer Eigenschaft als Verantwortliche, die Verpflichtungen nach dem Zakon za zashtita na lichnite danni (Gesetz zum Schutz personenbezogener Daten, im Folgenden: Datenschutzgesetz) und der Verordnung 2016/679 in hinreichendem Maß zu erfüllen, erlitten wurde.

Gegenstand und Rechtsgrundlage des Vorabentscheidungsersuchens

Vorabentscheidungsersuchen nach Art. 267 AEUV zur Auslegung der Erwägungsgründe 74, 85 und 146 sowie von Art. 4 Nr. 12, Art. 5 Abs. 2, Art. 24, 32 und 82 der Verordnung 2016/679.

Vorlagefragen

1. Sind Art. 24 und Art. 32 der Verordnung (EU) 2016/679 dahin auszulegen, dass es ausreicht, wenn eine unbefugte Offenlegung von beziehungsweise ein unbefugter Zugang zu personenbezogenen Daten im Sinne von Art. 4 Nr. 12 der Verordnung (EU) 2016/679 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 der Verordnung (EU) 2016/679 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 Verordnung (EU) 2016/679 dahin auszulegen, dass im Klageverfahren nach Art. 82 Abs. 1 der Verordnung (EU) 2016/679 der Verantwortliche die Beweislast dafür trägt, dass die getroffenen technischen und organisatorischen Maßnahmen nach Art. 32 der Verordnung 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 der Verordnung (EU) 2016/679 dahin auszulegen, dass die unbefugte Offenlegung von oder der unbefugte Zugang zu personenbezogenen Daten im Sinne von Art. 4 Nr. 12 der Verordnung (EU) 2016/679 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 Abs. 2 in Verbindung mit den Erwägungsgründen 85 und 146 der Verordnung (EU) 2016/679 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 Schadensersatz berechtigen, wenn ein solcher Missbrauch nicht festgestellt wurde und/oder kein weiterer Schaden der betroffenen Person entstanden ist?

Rechtsvorschriften und Rechtsprechung der Europäischen Union

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, im Folgenden: Verordnung): Erwägungsgründe 1, 4, 6, 74, 75, 76, 77, 83, 85, 146, Art. 4 Nrn. 2, 7 und 12, Art. 5, 24, 32, 33, 79, 82.

Urteil des Gerichtshofs vom 30. Mai 2013, Worten (C-342/12, EU:C:2013:355), Rn. 24 und 26.

Nationale Rechtsvorschriften

Administrativnoprotsesualen kodeks (Verwaltungsverfahrensordnung – Art. 144 Abs. 1, Art. 203 und 208).

Grazhdanski protsesualen kodeks (Zivilprozessordnung) – Art. 154.

Zakon za otgovornostta na darzhavata i obshtinite za vredi (Gesetz über die Haftung des Staates und der Gemeinden für Schäden) – Art. 1.

Zakon za zashtita na lichnite danni (Gesetz zum Schutz personenbezogener Daten) – Art. 39 Abs. 1 und 2, Art. 59 Abs. 1.

Kurze Darstellung des Sachverhalts und des Verfahrens

1 Die Natsionalna agentsia za prihodite (Nationale Agentur für Einnahmen, im Folgenden: NAP) ist Verantwortliche im Sinne von Art. 4 Nr. 7 der Verordnung. Nach dem nationalen Recht ist sie eine dem Finanzminister unterstellte Fachbehörde, zuständig für die Feststellung, Sicherung und Einziehung von öffentlichen und gesetzlich bestimmten privaten Staatsforderungen. In Erfüllung der ihr übertragenen öffentlichen Befugnisse verarbeitet sie personenbezogene Daten.

2 Am 15. Juli 2019 informierten die bulgarischen Medien die gesamte Gesellschaft darüber, dass ein unbefugter Zugang zum Informationssystem der NAP erfolgt sei und dass Informationen aus ihren Datenbanken, die personenbezogene Daten sowie Steuer- und Sozialversicherungsinformationen enthielten, im Internet veröffentlicht worden seien. Betroffen waren 4 057 328 bulgarische Staatsbürger, während sich die Anzahl aller betroffenen natürlichen Personen, zu denen sowohl bulgarische als auch ausländische Staatsbürger zählten, auf 6 074 140 belief. Unter den Betroffenen ist auch VB.

3 Bis zum jetzigen Zeitpunkt liegt keine rechtskräftige strafrechtliche Verurteilung der Personen vor, die den unbefugten, in den Medien als „Hackerangriff“ bezeichneten Zugang begangen haben [sollen].

4 Nach dem Zugang verklagten hunderte Bürger die NAP auf Ersatz des immateriellen Schadens.

5 Am 16. September 2019 erhob VB Klage gegen die NAP vor dem Administrativen sad Sofia-grad (Verwaltungsgericht der Stadt Sofia, im Folgenden: ASSG) auf Zahlung von Schadensersatz in Höhe von 1 000 Leva (BGN) (ca. 511 Euro) gemäß Art. 82 Abs. 1 der Verordnung, Art. 1 Abs. 1 des Gesetzes über die Haftung des Staates und der Gemeinden für Schäden (Zakon za otgovornostta na darzhavata i obshtinite za vredi) und Art. 39 Abs. 1 des Gesetzes zum Schutz personenbezogener Daten (Zakon za zashtita na lichnite danni).

6 In ihrer Klage im erstinstanzlichen Verfahren machte VB geltend, dass die NAP „nicht auf die bestmögliche Weise“ ihre Verpflichtung erfüllt habe, „ihre Cybersicherheit einwandfrei sicherzustellen“ und „in höchstem Maße die Sicherheit der personenbezogenen Daten der Staatsbürger der Republik Bulgarien wirksam zu gewährleisten“. Dadurch sei eine Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 der Verordnung eingetreten, und personenbezogene Daten seien unrechtmäßig offengelegt worden.

7 VB war der Ansicht, dass in „der mangelnden Sorgfalt und der Nichtanwendung von wirksamen Datenschutzmaßnahmen“ ein Unterlassen der NAP zu sehen sei, ihre Verpflichtungen zum Schutz der Daten der Bürger zu erfüllen und dass dies eine Verletzung der Art. 24 und 32 der Verordnung darstelle. Als Verantwortlicher sei die NAP verpflichtet, die personenbezogenen Daten in einer Weise zu verarbeiten, die „eine angemessene Sicherheit gewährleistet“, indem sie geeignete technische und organisatorische Maßnahmen umsetzt.

8 VB machte geltend, dass ihr durch die Pflichtverletzung der NAP ein immaterieller Schaden entstanden sei, der sich in Sorgen und Befürchtungen des künftigen Missbrauchs ihrer personenbezogenen Daten äußere, etwa dergestalt, dass ihr Vermögen enteignet werde, ihre Bankkonten missbraucht würden, Kredite in ihrem Namen abgeschlossen würden, ihr Personenstand geändert oder ihre Identität gestohlen werde. Sie ist empört über den „großen Einbruch in das Informationssystem der NAP“ und fühlt sich vom Staat nicht geschützt. Sie hat Angst, dass sie erpresst, angegriffen oder entführt werde.

9 Die NAP hielt die Klage für unbegründet. VB habe von der NAP keine Informationen darüber angefordert, zu welchen personenbezogenen Daten genau ein Zugriff erfolgte.

10 Nach dem erfolgten Zugang habe die NAP unverzüglich Maßnahmen zum Schutz der Rechte und Interessen der Bürger getroffen. Es hätten Treffen mit Vertretern und Experten der Sicherheitsdienste, der Notarialna kamara (Notarkammer), der Agentsia po vpisvaniata (Agentur für Eintragungen), der Asotsiatsia na targovskite banki (Verband der Handelsbanken) etc. stattgefunden, um die Maßnahmen zur Begrenzung der Folgen des Zugriffs zu koordinieren. Auf der

Webseite der NAP seien spezielle Rubriken über den Cyberangriff eingerichtet worden, in denen aktuelle Informationen veröffentlicht worden seien.

11 Nach Ansicht der NAP fehlt der kausale Zusammenhang zwischen dem behaupteten immateriellen Schaden und dem unberechtigten Zugang zu den personenbezogenen Daten. Die NAP sei Opfer eines mutwilligen Angriffs Dritter geworden, die nicht ihre Mitarbeiter seien. Daher sei sie für die eingetretenen Schäden nicht verantwortlich.

12 Die NAP machte geltend, dass sie zahlreiche Maßnahmen ergriffen habe. Sie habe nämlich Prozessmanagementsysteme und Managementsysteme für Informationssicherheit eingeführt, Verfahren genehmigt, die den internationalen Qualitätsnormen ISO 9000 und ISO 9001 entsprächen, sie wende Richtlinien, Regeln, Verfahren, Anweisungen und Methoden des Informationssicherheitsmanagements an.

13 Die NAP führte Beweismittel an, nämlich verschiedene interne Dokumente aus dem Zeitraum von Januar 2013 bis Mai 2019 über den Inhalt, das Verfahren zur Errichtung, Unterhaltung und über den Zugang zu den Datenbanken; die Einführung von Managementsystemen für Informationssicherheit; die Präventionsverfahren; die internen Regeln über die Netz- und Informationssicherheit; die Anweisungen über den Umgang mit Informationen; die Richtlinien zum Schutz personenbezogener Daten; die Maßnahmen und Mittel zum Schutz personenbezogener Daten; die Methoden und das Verfahren zur Risikobewertung.

14 Mit Urteil vom 27. November 2020 wies der ASSG die Klage von VB als unbegründet ab.

15 Der ASSG führte aus, dass der unbefugte Zugang zur Datenbank der NAP mittels eines „Hackerangriffs“ durch Personen erfolgt sei, gegen die ein Ermittlungsverfahren eingeleitet worden sei, das noch nicht abgeschlossen sei.

16 Das widerrechtliche Ergebnis lasse nicht vermuten, dass der Verantwortliche seine Verpflichtungen nicht erfüllt habe, geeignete technische und organisatorische Maßnahmen zur Sicherstellung des Schutzes der Datenbank zu treffen, so dass niemand in welcher Art und Weise und mit welchen Mitteln auch immer Zugang zu dieser Datenbank haben könne.

17 Der ASSG war der Auffassung, dass die Klägerin darlegen müsse, welche (technischen) Handlungen die NAP tatsächlich hätte vornehmen müssen, sie jedoch nicht oder schlecht ausgeführt habe, woraufhin das Ergebnis in Gestalt des unbefugten Zugangs zu und der Offenlegung von personenbezogenen Daten eingetreten sei oder wodurch zum Eintritt dieses Ergebnisses beigetragen worden sei.

18 Nach Auffassung des ASSG war unter Berücksichtigung der vorgelegten Beweismittel kein Unterlassen des Verantwortlichen festzustellen. VB sei kein

ersatzfähiger immaterieller Schaden entstanden. Die erlebte psychische Belastung, die durch die Nachricht vom unbefugten Zugang zu den Informationsdatenbanken der NAP ausgelöst worden sei, sei normal, stelle aber keinen tatsächlich entstandenen Schaden im rechtlichen Sinne dar. VB habe sich nicht dafür interessiert, zu genau welchen ihrer personenbezogenen Daten ein Zugang erlangt worden sei. Dieses Verhalten offenbare keinen starken emotionalen Stress.

19 Der ASSG befand, dass sich die öffentliche Bekanntmachung des erfolgten unrechtmäßigen Zugangs zu der Datenbank der NAP nicht auf das Leben von VB in Bezug auf ihr Selbstbewusstsein, ihr Selbstwertgefühl, ihre Arbeit, ihre Beziehungen und ihren Gesundheitszustand ausgewirkt habe. Es bestehe kein kausaler Zusammenhang mit den erlebten negativen Emotionen, da sie nicht das Ergebnis des Verhaltens der NAP seien.

20 VB hat das Urteil des ASSG bei dem vorlegenden Gericht, dem Varhoven administrativen sad (Oberstes Verwaltungsgericht, im Folgenden: VAS), angefochten.

Wesentliche Argumente der Parteien des Ausgangsverfahrens

21 In der Kassationsbeschwerde macht VB geltend, dass der ASSG die Beweislast hinsichtlich des Nachweises einer negativen Tatsache, nämlich des Unterlassens des Verantwortlichen, geeignete technische und organisatorische Maßnahmen zu treffen, unzutreffend verteilt habe.

22 VB ist der Ansicht, dass die Anwendung wirksamer Maßnahmen im Ermessen der NAP liege, so dass es nicht möglich sei, darzulegen, welche konkreten Verpflichtungen die Bediensteten der NAP hätten erfüllen müssen, dies jedoch unterlassen hätten. Die von der NAP vorgelegten Beweismittel hätten nicht nachgewiesen, dass die getroffenen technischen und organisatorischen Maßnahmen geeignet seien.

23 VB macht geltend, dass die Sorgen wegen eines möglichen künftigen Missbrauchs der personenbezogenen Daten keinen hypothetischen, sondern einen tatsächlichen immateriellen Schaden darstellten, der zu ersetzen sei. Es sei nicht erforderlich, einen gewöhnlichen immateriellen Schaden nachzuweisen.

24 Die NAP macht geltend, dass der ASSG zu Recht davon ausgegangen sei, dass sie in ihrer Eigenschaft als Verantwortliche kein Unterlassen begangen habe, sondern zahlreiche technische und organisatorische Maßnahmen zum Schutz bei der Verarbeitung personenbezogener Daten getroffen habe. Der tatsächliche Eintritt eines Schadens sei nicht nachgewiesen. Die Sorgen und die Angst vor zukünftigen Ereignissen seien nicht zu entschädigen.

Kurze Darstellung der Begründung der Vorlage

25 Ähnliche Gerichtsverfahren gegen die NAP endeten in erster Instanz mit widersprüchlichen Ergebnissen. Die Klagen wurden entweder als unbegründet abgewiesen oder aber ihnen wurde ganz oder teilweise stattgegeben. Die Rechtsvorschriften wurden in Bezug auf alle Elemente der Haftung des Verantwortlichen widersprüchlich ausgelegt und angewandt.

26 Der VAS ist der Auffassung, dass der Tatbestand der Haftung nach Art. 82 der Verordnung Folgendes umfasst: i) einen Verstoß des Verantwortlichen gegen diese Verordnung; ii) einen materiellen oder immateriellen Schaden, der der betroffenen Person entstanden ist, und iii) einen kausalen Zusammenhang zwischen dem entstandenen Schaden und dem konkreten Verstoß.

Erste Frage

27 Nach Art. 24 Abs. 1 der Verordnung setzt der Verantwortliche 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.

28 Art. 32 der Verordnung sieht Verpflichtungen des Verantwortlichen im Zusammenhang mit der Sicherheit der Verarbeitung vor, die für seine Verantwortung nach Art. 24 relevant sind und sie auslösen, wobei die Kriterien aufgezählt werden, nach denen die geeigneten technischen und organisatorischen Maßnahmen anzuwenden sind, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dazu zählen „der Stand der Technik, die Implementierungskosten und die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen“.

29 Die Verordnung definiert den Begriff „geeignete technische und organisatorische Maßnahmen“ nicht. Im 74. Erwägungsgrund wird angegeben, dass der Verantwortliche geeignete und wirksame Maßnahmen treffen muss und nachweisen können sollte, dass die Verarbeitungstätigkeiten im Einklang mit der Verordnung stehen und die Maßnahmen auch wirksam sind.

30 Das Vorstehende führt zu dem Schluss, dass der Verantwortliche eine Risikobewertung nach den in Art. 32 der Verordnung festgelegten Kriterien durchzuführen hat, auf deren Grundlage er technische und organisatorische Maßnahmen zu treffen hat, die im Hinblick auf das erforderliche und dem Risiko angemessene Schutzniveau für die personenbezogenen Daten geeignet sind. Durch die Einführung geeigneter technischer und organisatorischer Maßnahmen stellt der Verantwortliche sicher, dass er personenbezogene Daten im Einklang mit der Verordnung verarbeitet.

31 Aus den genannten Rechtsvorschriften folgt, dass die Wahl der geeigneten technischen und organisatorischen Maßnahmen eine Frage der Zweckmäßigkeit ist. Die Beurteilung der Zweckmäßigkeit durch den Verantwortlichen unterliegt jedoch keiner gerichtlichen Überprüfung, da das Gericht die Rechtmäßigkeit überprüft. Gleichzeitig hat die Verarbeitung personenbezogener Daten bei bestehendem Ermessensspielraum bezüglich der Auswahl der technischen und organisatorischen Maßnahmen im Rahmen der Verordnung und unter Einhaltung des Ziels zu erfolgen, das Grundrecht auf Schutz der personenbezogenen Daten natürlicher Personen zu wahren.

32 Unter Berücksichtigung des oben Dargelegten ersucht der VAS um Klärung, ob die Art. 24 und 32 der Verordnung dahin auszulegen sind, dass allein der Eintritt eines rechtswidrigen Ergebnisses in Gestalt einer unbefugten Offenlegung von beziehungswiese eines unbefugten Zugangs zu personenbezogenen Daten im Sinne von Art. 4 Nr. 12 der Verordnung nachweist, dass die vom Verantwortlichen getroffenen technischen und organisatorischen Maßnahmen nicht geeignet waren.

Zweite Frage (bei Verneinung der ersten Frage)

33 Da die Auswahl und die Anwendung von technischen und organisatorischen Maßnahmen der subjektiven Beurteilung des Verantwortlichen überlassen wurden und in seinen Ermessensspielraum fallen, stellt sich für den VAS die Frage, welchen Gegenstand und Umfang die gerichtliche Rechtmäßigkeitskontrolle bei der Prüfung haben sollte, ob die vom Verantwortlichen getroffenen technischen und organisatorischen Maßnahmen geeignet sind und den Art. 24 und 32 der Verordnung entsprechen.

34 Der VAS hat Zweifel, ob es ausreicht, wenn das Gericht feststellt, in welcher Weise der Verantwortliche die aus den genannten Vorschriften folgenden Verpflichtungen erfüllt hat, oder ob es die getroffenen und umgesetzten technischen und organisatorischen Maßnahmen inhaltlich prüfen muss, die jedoch in der Verordnung lediglich beispielhaft angeführt werden und je nach Zweckmäßigkeit umgesetzt werden.

Dritte Frage (bei Verneinung der ersten Frage)

35 Nach Art. 5 Abs. 2 der Verordnung ist der Verantwortliche für die Einhaltung der Grundsätze des Absatzes 1 derselben Bestimmung, die die Verarbeitung personenbezogener Daten betreffen, verantwortlich und muss deren Einhaltung nachweisen können. Art. 24 Abs. 1 der Verordnung verpflichtet den Verantwortlichen, „geeignete technische und organisatorische Maßnahmen umzusetzen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt“.

36 Art. 82 Abs. 3 der Verordnung ermöglicht es dem Verantwortlichen oder dem Auftragsverarbeiter, sich von der Haftung gemäß Absatz 2 zu befreien, „wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist“. Nach dem genannten Absatz 2 haftet der Verantwortliche für den Schaden, der durch eine nicht der Verordnung entsprechende Verarbeitung verursacht wurde.

37 Nach dem nationalen Recht ist jede Partei eines Klageverfahrens verpflichtet, die Umstände, aus denen sie ihre Ansprüche oder Einwendungen herleitet, nachzuweisen. In den gleichgelagerten Verfahren haben die erstinstanzlichen Gerichte die Beweislast zwischen Kläger und Beklagtem unterschiedlich verteilt.

38 Im vorliegenden Fall ist die Frage relevant, ob der Grundsatz der Rechenschaftspflicht nach Art. 5 Abs. 2 in Verbindung mit dem 74. Erwägungsgrund und Art. 24 Abs. 1 der Verordnung dahin auszulegen ist, dass sie die Beweislast umkehren und der Verantwortliche, gegen den eine Schadensersatzklage wegen eines Verstoßes gegen die Verordnung erhoben wurde, als Beklagter verpflichtet ist, nachzuweisen, dass die von ihm angewandten technischen und organisatorischen Maßnahmen geeignet sind.

39 Neben der Frage nach dem Gegenstand und dem Umfang der gerichtlichen Überprüfung der Erfüllung der Verpflichtungen aus der Verordnung ist es auch problematisch, wie und anhand welcher Beweismittel überprüft werden soll, ob sie erfüllt wurden und insbesondere ob alle geeigneten technischen und organisatorischen Maßnahmen angewandt wurden.

40 Im Verfahren legte die NAP Beweismittel hinsichtlich der Gewährleistung des Schutzes der Informationsnetze nach den in den Dokumenten angegebenen Standards vor, aber es wurde kein forensisch-technisches Sachverständigengutachten eingeholt, um festzustellen, ob die technischen und organisatorischen Maßnahmen geeignet im Sinne der Verordnung waren. Der VAS ist sich bewusst, dass ein Verantwortlicher wie die NAP verpflichtet ist, organisatorische, technologische und technische Maßnahmen für Netz- und Informationssicherheit anzuwenden, die in einem angemessenen Verhältnis zu den Bedrohungen durch die Cyberkriminalität stehen, um das Risiko ihrer Verwirklichung zu minimieren. Allerdings könnte der Zugang von forensischen Sachverständigen in jedem Verfahren, dessen Rechtsgrundlage Art. 82 der Verordnung ist, neue negative Folgen für den Schutz personenbezogener Daten haben.

41 Unter Berücksichtigung des Stands der Technik, der existierenden Standards zum Schutz der Informationsnetzsysteme und des erfolgten unbefugten Zugangs mittels eines „Hackerangriffs“ durch Personen, die sich außerhalb der Verwaltung des Verantwortlichen befinden, stellt sich der VAS die Frage, ob die Einholung eines forensisch-technischen Sachverständigengutachtens durch das Gericht als ein notwendiges und ausreichendes Beweismittel angesehen werden kann, um festzustellen, ob die getroffenen und angewandten technischen und

organisatorischen Maßnahmen geeignet waren, den Schutz der personenbezogenen Daten sicherzustellen.

Vierte Frage

42 Als an einer Verarbeitung beteiligter Verantwortlicher haftet die NAP, kann sich aber von der Haftung gemäß Art. 82 Abs. 3 befreien, wenn sie nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

43 Im Verfahren ist es unstreitig, dass der Zugang zu den personenbezogenen Daten mittels eines „Hackerangriffs“ gegen die NAP stattfand. Hingegen erfolgten der unbefugte Zugang zu und die Offenlegung von personenbezogenen Daten nicht bei beziehungsweise anlässlich der Verarbeitung personenbezogener Daten durch Mitarbeiter der NAP.

44 Der VAS ersucht um Feststellung, ob im vorliegenden Fall die Annahme möglich ist, dass ein Umstand vorliegt, für den der Verantwortliche in keinerlei Hinsicht verantwortlich ist und dass dieser Umstand ihn dem entsprechend von der Haftung befreit.

Fünfte Frage

45 Die betroffene Person begehrt Ersatz des immateriellen Schadens, der sich in Sorgen, Angst, Stress, Unsicherheitsgefühlen und Befürchtungen eines künftigen Missbrauchs ihrer personenbezogenen Daten in von ihr beschriebener unterschiedlicher Art und Weise äußert. Es liegen keine Anhaltspunkte vor, dass mit den personenbezogenen Daten von VB Missbrauch betrieben wurde.

46 Wie aus den Erwägungsgründen 75 und 85 der Verordnung hervorgeht, werden bei der Aufzählung von Beispielen materieller oder immaterieller Schäden die Art der personenbezogenen Daten und die nachteiligen Auswirkungen für die betroffenen Personen und nicht nur ihr subjektives Empfinden berücksichtigt.

47 Im 146. Erwägungsgrund der Verordnung wird die Grenze der Haftung festgelegt. Diese umfasst „die Schäden“, die einer Person aufgrund einer Verarbeitung entstehen, die mit der Verordnung nicht im Einklang steht.

48 Nachdem bereits ein Zugang erfolgte, können die personenbezogenen Daten der betroffenen Person Gegenstand zahlreicher Missbrauchsfälle immaterieller und materieller Art mit erheblichen Auswirkungen werden. In der Öffentlichkeit sind solche Missbrauchsfälle bekannt geworden, was eine höhere Besorgnis der durch den „Hackerangriff“ betroffenen Personen begründen kann. Im vorliegenden Fall ist der künftige Missbrauch aufgrund fehlender Angaben über einen bereits erfolgten Missbrauch lediglich eine Vermutung, eine Hypothese mit einem möglichen, aber ungewissen Risiko für die Rechte der betroffenen Person.

49 Aus den dargelegten Gründen stellt sich die Frage, ob die negativen Empfindungen der betroffenen Person in diesem Kontext, d. h. ob allein die Tatsache, dass Gefahr eines möglichen künftigen Missbrauchs der personenbezogenen Daten entstanden ist, unter den weit auszulegenden Begriff des immateriellen Schadens fällt und einen Entschädigungsgrund nach Art. 82 Abs. 1 in Verbindung mit dem 146. Erwägungsgrund der Verordnung darstellt.

50 Es ist jedoch möglich, dass Art. 82 Abs. 1 in Verbindung mit dem 146. Erwägungsgrund der Verordnung nicht dahin ausgelegt werden kann, dass jede negative Empfindung, Angst oder Sorge der betroffenen Person zum Ersatz des entstandenen immateriellen Schadens berechtigt, wenn zuvor keine unrechtmäßige Nutzung wie beispielsweise durch Enteignung von Vermögen, Abschluss von Krediten im Namen der betroffenen Person oder Identitätsdiebstahl erfolgt ist.