Sammlung der Rechtsprechung

SCHLUSSANTRÄGE DES GENERALANWALTS
GIOVANNI PITRUZZELLA
vom 27. April 2023[1]

Rechtssache C-340/21

VB
gegen
Natsionalna agentsia za prihodite

(Vorabentscheidungsersuchen des Varhoven administrativen sad [Oberstes Verwaltungsgericht, Bulgarien])

„Vorlage zur Vorabentscheidung – Schutz personenbezogener Daten – Verordnung (EU) 2016/679 – Haftung des Verantwortlichen – Sicherheit der Verarbeitung – Verletzung der Sicherheit der Verarbeitung personenbezogener Daten – Immaterieller Schaden wegen Unterlassens durch den Verantwortlichen – Schadensersatzklage“

Kann die unrechtmäßige Verbreitung personenbezogener Daten, die sich im Besitz einer öffentlichen Behörde befinden, aufgrund eines Hackerangriffs zu einem Ersatz des immateriellen Schadens zugunsten eines Dateninhabers führen, und zwar allein deshalb, weil dieser einen möglichen künftigen Missbrauch seiner Daten befürchtet? Nach welchen Kriterien kann der Verantwortliche haftbar gemacht werden? Wie ist die Beweislast innerhalb eines gerichtlichen Verfahrens verteilt? In welchem Umfang erfolgt die gerichtliche Prüfung?

I. Rechtlicher Rahmen

1. Art. 4 („Begriffsbestimmungen“) der Verordnung 2016/679[2] (im Folgenden: Verordnung) bestimmt:

„Im Sinne dieser Verordnung bezeichnet der Ausdruck:

…

[1] Originalsprache: Italienisch.

[2] 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).

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;

…"

2. Art. 5 („Grundsätze für die Verarbeitung personenbezogener Daten") sieht vor:

„(1) Personenbezogene Daten müssen

…

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')".

3. Art. 24 („Verantwortung des für die Verarbeitung Verantwortlichen") der Verordnung 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".

4. Art. 32 („Sicherheit der Verarbeitung") 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 gegebenenfalls unter anderem Folgendes ein:

…

(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.

…“

5. Art. 82 der Verordnung „Haftung und Recht auf Schadenersatz“ bestimmt Folgendes:

„(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“.

II. Sachverhalt, Ausgangsverfahren und Vorlagefragen

6. Am 15. Juli 2019 veröffentlichten die bulgarischen Medien die Nachricht, dass ein unbefugter Zugang zum Informationssystem der Natsionalna agentsia za prihodite (Nationale Agentur für Einnahmen, Bulgarien, im Folgenden: NAP[3]) erfolgt sei und dass verschiedene Steuer- und Sozialversicherungsdaten von Millionen von Menschen, sowohl bulgarischen als auch ausländischen Staatsbürgern, im Internet veröffentlicht worden seien.

7. Mehrere Personen, darunter VB, die Klägerin des Ausgangsverfahrens, verklagten daher die NAP auf Ersatz des immateriellen Schadens.

8. Im vorliegenden Fall erhob die Klägerin des Ausgangsverfahrens Klage vor dem Administrativen sad Sofia-grad (Verwaltungsgericht der Stadt Sofia, Bulgarien, im Folgenden: ASSG) und machte geltend, dass die NAP gegen nationale Vorschriften sowie gegen ihre Verpflichtung verstoßen habe, als Verantwortliche personenbezogene Daten in einer Weise zu verarbeiten, die „angemessene Sicherheitsstandards gewährleistet“, indem sie geeignete technische und organisatorische Maßnahmen gemäß den Art. 24 und 32 der Verordnung Nr. 679/2016 umsetze. Die Klägerin machte geltend, dass ihr ein immaterieller Schaden entstanden sei, der sich in Sorgen und Befürchtungen des künftigen Missbrauchs ihrer personenbezogenen Daten äußere.

[3] Die 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 Abgaben und zuständig für die Feststellung, Sicherung und Einziehung von gesetzlich bestimmten öffentlichen und privaten Staatsforderungen. Bei der Ausübung der ihr übertragenen öffentlichen Befugnisse verarbeitet sie personenbezogene Daten.

9. Die Gegenpartei machte geltend, die Klägerin habe im Ausgangsverfahren keine Informationen darüber angefordert, auf welche personenbezogenen Daten genau zugegriffen worden sei. Nach Bekanntwerden des Zugriffs habe die NAP ein Treffen von Führungskräften mit Experten einberufen, um die Rechte und Interessen der Bürger zu schützen. Darüber hinaus fehlt nach Ansicht der NAP der kausale Zusammenhang zwischen dem unberechtigten Zugriff und dem behaupteten immateriellen Schaden, da die NAP alle Prozessmanagementsysteme und Managementsysteme für Informationssicherheit eingeführt habe, die den geltenden internationalen Datenschutzbestimmungen entsprächen.

10. Das erstinstanzliche Gericht, der ASSG, wies die Klage mit der Begründung ab, dass die Veröffentlichung der Daten nicht der NAP zuzurechnen sei, dass die Beweislast für die Geeignetheit der getroffenen Maßnahmen bei der Klägerin liege und dass kein immaterieller Schaden geltend gemacht werden könne.

11. Gegen das erstinstanzliche Urteil wurde anschließend beim Varhoven administrativen sad (Oberstes Verwaltungsgericht, Bulgarien) Kassationsbeschwerde eingelegt. Die Klägerin des Ausgangsverfahrens hat u. a. geltend gemacht, dass das erstinstanzliche Gericht die Beweislast hinsichtlich des Unterlassens der Anwendung von Sicherheitsmaßnahmen falsch verteilt habe. Auch der immaterielle Schaden sollte nicht Gegenstand der Beweislast sein, da es sich um einen tatsächlichen und nicht nur um einen möglichen immateriellen Schaden handele.

12. Die NAP machte ihrerseits geltend, notwendige technische und organisatorische Maßnahmen in ihrer Eigenschaft als für die Datenverarbeitung Verantwortliche getroffen zu haben, und bestritt das Vorliegen eines Beweises für einen tatsächlichen immateriellen Schaden. Bei Angst und Befürchtungen handele es sich um nicht ersatzfähige emotionale Zustände.

13. Das vorlegende Gericht stellte fest, dass die einzelnen Verfahren, die die Geschädigten getrennt gegen die NAP auf Ersatz des immateriellen Schadens angestrengt hätten, zu unterschiedlichen Ergebnissen geführt hätten.

14. Das vorlegende Gericht hat daher das Verfahren ausgesetzt und dem Gerichtshof folgende Vorlagefragen zur Vorabentscheidung vorgelegt:

1. Sind 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) 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 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 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?

III. Rechtliche Würdigung

A. Vorbemerkungen

15. In der vorliegenden Rechtssache geht es um interessante und zum Teil erstmals aufgeworfene Fragen bezüglich der Auslegung verschiedener Bestimmungen der Verordnung [4].

16. Bei den fünf Vorlagefragen geht es um dieselbe Frage: die Bedingungen für den Ersatz des immateriellen Schadens einer Person, deren personenbezogene Daten, die sich im Besitz einer öffentlichen Agentur befinden, nach einem Hackerangriff im Internet veröffentlicht wurden.

17. Der Einfachheit halber schlage ich vor, alle Fragen in der Reihenfolge der Vorlageentscheidung getrennt zu beantworten, auch wenn ich mir dessen bewusst bin, dass es einige konzeptuelle Überschneidungen gibt, da die ersten vier darauf abzielen, die

[4] Art. 5 Abs. 2 (betreffend den Grundsatz der Verantwortung jedes für die Verarbeitung personenbezogener Daten Verantwortlichen), Art. 24 (betreffend die Maßnahmen, die der Verantwortliche umsetzen muss, um sicherzustellen, dass die Verarbeitung gemäß dieser Verordnung erfolgt), Art. 32 (betreffend diese Verpflichtung insbesondere in Bezug auf die Sicherheit der Verarbeitung) und Art. 82 Abs. 1 bis 3 (betreffend den Schadensersatz bei Verstößen gegen diese Verordnung und die Möglichkeit des Verantwortlichen, Maßnahmen zu treffen, um die Einhaltung dieser Verordnung zu gewährleisten) sowie die Erwägungsgründe 74, 85 und 146, die mit den vorgenannten Artikeln in Verbindung stehen.

Voraussetzungen für die Verantwortung des Verantwortlichen für den Verstoß gegen die Bestimmungen der Verordnung zu ermitteln [5] und die fünfte sich auf den Begriff des immateriellen Schadens für die Zwecke des Schadensersatzes bezieht [6].

18. Ich möchte darauf hinweisen, dass beim Gerichtshof derzeit mehrere Rechtssachen zu Art. 82 der Verordnung anhängig sind und dass in einer dieser Rechtssachen bereits die Schlussanträge des Generalanwalts verlesen wurden, die ich in dieser Analyse berücksichtigen werde [7].

19. Bevor ich auf die aufgeworfenen Fragen eingehe, halte ich es für angebracht, einige Überlegungen zu den Grundsätzen und Zielen der Verordnung anzustellen, die für die Beantwortung der einzelnen Fragen von Nutzen sein werden.

20. Art. 24 der Verordnung legt allgemein fest, dass der Verantwortliche geeignete technische und organisatorische Maßnahmen umsetzen muss, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß der Verordnung erfolgt, während Art. 32 der Verordnung die gleiche Verpflichtung speziell für die Sicherheit der Verarbeitung festlegt. Die Art. 24 und 32 beschreiben genauer das, was bereits in Art. 5 Abs. 2 vorgesehen ist, der unter die „Grundsätze für die Verarbeitung personenbezogener Daten" den Grundsatz der „Rechenschaftspflicht" einführt. Dieser ergibt sich logischerweise aus dem in Art. 5 Abs. 1 Buchst. f verankerten Grundsatz der „Integrität und Vertraulichkeit" und ergänzt diesen, so dass beide im Licht des risikobasierten Ansatzes, auf dem die Verordnung beruht, verstanden werden müssen.

21. Der Grundsatz der Rechenschaftspflicht ist einer der Eckpfeiler der Verordnung und eine ihrer wichtigsten Neuerungen. Er legt dem Verantwortlichen die Verantwortung auf, aktiv Maßnahmen zu ergreifen, um die Einhaltung der Verordnung zu gewährleisten, und bereit zu sein, diese nachzuweisen [8].

22. In der Lehre wurde von einem echten kulturellen Wandel gesprochen, der sich aus der „globalen Reichweite der Rechenschaftspflicht" ergibt [9]. Es geht nicht so sehr um die formale Einhaltung der rechtlichen Verpflichtung oder der einzelnen Maßnahme, sondern um die angewandte Gesamtstrategie des Unternehmens, die den Verantwortlichen von der Haftung befreit, weil er die Datenschutzvorschriften einhält.

[5] a) Die erste zielt auf die Beantwortung der Frage ab, ob das bloße Vorliegen einer Verletzung der Systeme dazu führen kann, die angewandten Maßnahmen als ungeeignet zu beurteilen; b) die zweite betrifft die Frage, in welchem Umfang das Gericht prüfen kann, ob diese Maßnahmen geeignet waren; c) die dritte bezieht sich auf die Beweislast im Zusammenhang mit der Prüfung, ob die Maßnahmen geeignet waren, sowie auf einige technische Modalitäten bei der Suche nach Beweisen; d) bei der vierten geht es um die Frage, ob der Umstand, dass der Angriff auf das System von außen kommt, für die Haftungsbefreiung relevant ist.

[6] Was die genannten Bestimmungen der Verordnung betrifft, so geht es bei den ersten drei Fragen um die Verantwortung des Verantwortlichen in Bezug auf die Frage, ob die zu treffenden Maßnahmen geeignet sind (Art. 5, 24 und 32); die vierte und die fünfte Frage betreffen die Voraussetzungen für die Haftungsbefreiung und den Begriff des ersatzfähigen immateriellen Schadens (Art. 82).

[7] Vgl. Schlussanträge des Generalanwalts Campos Sánchez-Bordona in der Rechtssache Österreichische Post (Immaterieller Schaden im Zusammenhang mit der Verarbeitung personenbezogener Daten) (C-300/21, EU:C:2022:756).

[8] C. Docksey, *Article 24. Responsibility of the controller*, in C. Kuner, L. A. Bygrave, C. Docksey, L. Drechsler, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, 2020, S. 561. Die Grundsätze und Verpflichtungen der Datenschutzbestimmungen sollten das kulturelle Gefüge von Organisationen auf allen Ebenen prägen und nicht als eine Reihe rechtlicher Anforderungen betrachtet werden, die von der Rechtsabteilung abgehakt werden müssen.

[9] E. Belisario, G. Riccio, G. Scorza, *GDPR e Normativa Privacy – Commentario*, Wolters Kluwer, 2022, S. 301.

23. Die vom Grundsatz der Rechenschaftspflicht geforderten technischen und organisatorischen Maßnahmen müssen unter Berücksichtigung der in Art. 24 genannten Faktoren „geeignet" sein: Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen.

24. Art. 24 verlangt daher, dass die Maßnahmen geeignet sind, um nachweisen zu können, dass die Verarbeitung im Einklang mit den Grundsätzen und Bestimmungen der Verordnung erfolgt.

25. Art. 32 hingegen projiziert den Grundsatz der Rechenschaftspflicht auf die konkreten Maßnahmen, die zu treffen sind, um „ein dem Risiko angemessenes Schutzniveau zu gewährleisten". Damit werden die bereits vorgesehenen Faktoren, die bei der Umsetzung der technischen und organisatorischen Maßnahmen zu berücksichtigen sind, um den Stand der Technik und die Implementierungskosten ergänzt.

26. Der Begriff „geeignet" setzt voraus, dass die zur Sicherung der Informationssysteme gewählten Maßnahmen sowohl in technischer (Angemessenheit der Maßnahmen) als auch in qualitativer Hinsicht (Wirksamkeit des Schutzes) ein akzeptables Niveau erreichen. Um die Einhaltung der Grundsätze der Notwendigkeit, Angemessenheit und Verhältnismäßigkeit zu gewährleisten, muss die Verarbeitung nicht nur geeignet sein, sondern auch den Zwecken entsprechen, denen sie dienen soll. Dabei spielt der Grundsatz der Minimierung eine entscheidende Rolle, wonach auf allen Stufen der Datenverarbeitung stets darauf geachtet werden muss, dass Sicherheitsrisiken minimiert werden [10].

27. Die gesamte Verordnung verfolgt das Ziel, Risiken vorzubeugen und den Verantwortlichen in die Pflicht zu nehmen, und verfolgt daher einen teleologischen Ansatz, der auf das bestmögliche Ergebnis in Bezug auf die Wirksamkeit abzielt, d. h. weit entfernt von formalistischer Logik, die mit der bloßen Verpflichtung zur Einhaltung bestimmter Verfahren verbunden ist, die dazu dienen, sich von der Haftung zu befreien [11].

28. Art. 24 enthält keine erschöpfende Aufzählung „geeignet[er]" Maßnahmen: Diese müssen von Fall zu Fall beurteilt werden. Dies steht im Einklang mit der Philosophie der Verordnung, aus der hervorgeht, dass die zu wählenden Verfahren auf der Grundlage einer sorgfältigen Bewertung der spezifischen Situation auszuwählen sind, um möglichst wirksam zu sein [12].

[10] E. Belisario, G. Riccio, G. Scorza, *GDPR*, oben angeführt, S. 380.

[11] Daher können, wie wir sehen werden, die erste und die vierte Vorlagefrage nur verneint werden. Aus den Bestimmungen der Verordnung lässt sich kein Automatismus ableiten: Weder reicht die bloße Tatsache, dass eine Offenlegung personenbezogener Daten stattgefunden hat, aus, um anzunehmen, dass die getroffenen technischen und organisatorischen Maßnahmen nicht geeignet sind, noch reicht die Tatsache, dass die Offenlegung durch das Eingreifen von Personen außerhalb der Organisation des Verantwortlichen und außerhalb seines Kontrollbereichs erfolgt ist, aus, um ihn von der Haftung zu befreien.

[12] L. Bolognini, E. Pelino, *Codice della disciplina privacy*, Giuffrè, 2019, S. 201. Der Unionsgesetzgeber geht damit über die Konzeption der Sicherheit der Verarbeitung hinaus, die auf dem Vorhandensein von vorab festgelegten Sicherheitsmaßnahmen basiert, und wendet eine Methodik an, die für die internationalen Standards im Bereich der Verwaltung von risikobasierten Informationssystemen typisch ist: Sie sieht die Ermittlung von Maßnahmen zur Risikominderung vor, die über vorkonfigurierte und allgemein anwendbare Checklisten hinausgehen. Daher müssen internationale Richtlinien und Standards herangezogen werden. Das Ergebnis dieser Risikobewertung wird dann verbindlich, wenn die Organisation Entscheidungen trifft, um die festgestellten Risiken zu mindern, und sich damit selbst rechenschaftspflichtig macht.

B. Erste Vorlagefrage

29. Mit der ersten Frage möchte das vorlegende Gericht im Wesentlichen wissen, ob die Art. 24 und 32 der Verordnung dahin auszulegen sind, dass das Vorliegen einer „Verletzung des Schutzes personenbezogener Daten" im Sinne von Art. 4 Nr. 12 der Verordnung an sich ausreicht, um anzunehmen, dass die vom Verantwortlichen ergriffenen technischen und organisatorischen Maßnahmen nicht „geeignet" waren, um den Schutz der Daten zu gewährleisten.

30. Aus dem Wortlaut der Art. 24 und 32 der Verordnung ergibt sich, dass der Verantwortliche bei der Auswahl der technischen und organisatorischen Maßnahmen, die er zur Einhaltung der Verordnung zu treffen hat, eine Reihe von Bewertungsfaktoren berücksichtigen muss, die in diesen und den oben angeführten Artikeln aufgezählt sind.

31. Der Verantwortliche verfügt über ein gewisses Ermessen bei der Auswahl der Maßnahmen, die in Anbetracht seiner spezifischen Situation am besten geeignet sind; diese Entscheidung unterliegt jedoch einer möglichen gerichtlichen Prüfung der Vereinbarkeit der angewandten Maßnahmen mit allen sich aus der Verordnung ergebenden Verpflichtungen und den mit ihr verfolgten Zielen.

32. Insbesondere in Bezug auf die Sicherheitsmaßnahmen muss der Verantwortliche gemäß Art. 32 Abs. 1 den „Stand der Technik" berücksichtigen. Dies impliziert eine Begrenzung des technologischen Niveaus der durchzuführenden Maßnahmen auf das, was zum Zeitpunkt des Ergreifens der Maßnahmen vernünftigerweise möglich ist, d. h., die Eignung der Maßnahme zur Gefahrenabwehr muss in einem angemessenen Verhältnis zu den Lösungen stehen, die der aktuelle Stand von Wissenschaft, Technik, Technologie und Forschung bietet, wobei, wie noch zu zeigen sein wird, auch die Implementierungskosten zu berücksichtigen sind.

33. Maßnahmen können zu einem bestimmten Zeitpunkt „geeignet" sein und trotzdem von Cyberkriminellen umgangen werden, die über sehr ausgeklügelte Instrumente verfügen, mit denen sie selbst modernste Sicherheitsmaßnahmen aushebeln können.

34. Es erscheint unlogisch, anzunehmen, dass es die Absicht des Unionsgesetzgebers war, dem Verantwortlichen die Verpflichtung aufzuerlegen, jede Verletzung personenbezogener Daten zu verhindern, unabhängig von der Sorgfalt, die er bei der Ausarbeitung der Sicherheitsmaßnahmen anwenden muss [13].

35. Wie bereits erwähnt, rückt die Verordnung vom Automatismus ab und verlangt von dem Verantwortlichen ein hohes Maß an Verantwortung, was jedoch nicht dazu führen darf, dass diesem die Möglichkeit genommen wird, nachweisen zu können, dass er die ihm auferlegten Pflichten ordnungsgemäß erfüllt hat.

36. Darüber hinaus bestimmt Art. 32 Abs. 1, dass die „Implementierungskosten" der in Frage kommenden technischen und organisatorischen Maßnahmen berücksichtigt werden müssen. Daraus folgt, dass die Beurteilung der Geeignetheit solcher Maßnahmen auf einer Abwägung zwischen den Interessen der betroffenen Person, die generell ein höheres Schutzniveau

[13] Der Begriff „geeignet" zeigt unmissverständlich die Absicht, nicht allen abstrakt möglichen technischen und organisatorischen Maßnahmen Bedeutung beizumessen. In diesem Sinne M. Gambini, *Responsabilità e risarcimento nel trattamento dei dati personali*, in V. Cuffaro, R. D'Orazio, V. Ricciuto, *I dati personali nel diritto europeo*, Giappichelli, 2019, S. 1059.

anstreben, und den wirtschaftlichen Interessen und technischen Möglichkeiten des Verantwortlichen, die zuweilen ein niedrigeres Schutzniveau anstreben, beruhen muss. Diese Abwägung muss den Anforderungen des allgemeinen Verhältnismäßigkeitsgrundsatzes genügen.

37. Im Licht einer systematischen Auslegung ist hinzuzufügen, dass der Gesetzgeber die Möglichkeit von Systemverletzungen berücksichtigt hat; Art. 32 Abs. 1 Buchst. c bezieht unter den vorgeschlagenen Maßnahmen die Fähigkeit ein, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen. Die Bereitstellung von Sicherheitsmaßnahmen, die ein dem Risiko einer solchen Fähigkeit angemessenes Schutzniveau gewährleisten, wäre nutzlos, wenn man davon ausginge, dass allein die Verletzung von Systemen als Beweis dafür ausreichen würde, dass die Maßnahmen ungeeignet sind.

C. Zweite Vorlagefrage

38. Mit der zweiten Frage möchte das vorlegende Gericht im Wesentlichen wissen, welchen Gegenstand und Umfang die gerichtliche Kontrolle bei der Prüfung haben sollte, ob die von dem für die Verarbeitung personenbezogener Daten Verantwortlichen getroffenen technischen und organisatorischen Maßnahmen nach Art. 32 der Verordnung geeignet sind.

39. Angesichts der unterschiedlichen Situationen, die in der Praxis auftreten können, enthält die Verordnung, wie bereits erwähnt, keine verbindlichen Vorschriften für die Bestimmung der technischen und organisatorischen Maßnahmen, die der Verantwortliche zu treffen hat, um die Anforderungen der Verordnung zu erfüllen. Die Frage, ob die ergriffenen Maßnahmen geeignet sind, muss daher konkret beurteilt werden, wobei zu prüfen ist, ob die spezifischen Maßnahmen geeignet waren, das Risiko in angemessener Weise zu verhindern und die negativen Auswirkungen des Verstoßes zu minimieren.

40. Auch wenn es zweifellos zutrifft, dass die Auswahl und Umsetzung solcher Maßnahmen unter die subjektive Beurteilung des Verantwortlichen fällt, kann sich die Prüfung des Gerichts nicht darauf beschränken, zu überprüfen, ob der Verantwortliche seinen Verpflichtungen aus den Art. 24 und 32 nachkommt, d. h., ob er (formal) bestimmte technische und organisatorische Maßnahmen vorgesehen hat. Es muss den Inhalt dieser Maßnahmen, die Art und Weise ihrer Umsetzung und ihre praktischen Auswirkungen auf der Grundlage der ihm zur Verfügung stehenden Beweismittel und der Umstände des Einzelfalls konkret prüfen. Wie die portugiesische Regierung zutreffend festgestellt hat, „scheint die Art und Weise, in der er seinen Verpflichtungen nachgekommen ist, untrennbar vom Inhalt der getroffenen Maßnahmen zu sein, um nachzuweisen, dass der Verantwortliche unter Berücksichtigung des spezifischen Datenverarbeitungsvorgangs (seiner Art, seines Umfangs, seines Zusammenhangs und seiner Zwecke), des Stands der Technik der verfügbaren Technologien und ihrer Kosten sowie der Risiken für die Rechte und Freiheiten der Bürger alle erforderlichen und geeigneten Maßnahmen ergriffen hat, um ein dem zugrunde liegenden Risiko angemessenes Sicherheitsniveau zu garantieren“ [14].

41. Bei der gerichtlichen Prüfung müssen daher alle Faktoren berücksichtigt werden, die in den Art. 24 und 32 enthalten sind und in denen, wie bereits erwähnt, eine Reihe von Kriterien angeführt ist, um beurteilen zu können, ob die Maßnahmen geeignet sind, sowie Beispiele für Maßnahmen genannt werden, die als geeignet beurteilt werden können. Wie die Kommission

[14] Schriftliche Erklärungen, Rn. 31.

und alle Mitgliedstaaten, die zur zweiten Frage Stellung genommen haben, betont haben, wird in Art. 32 Abs. 1 bis 3 die Notwendigkeit hervorgehoben, „ein dem Risiko angemessenes Schutzniveau zu gewährleisten“, wobei auf andere Faktoren verwiesen wird, die für diesen Zweck von Bedeutung sind, z. B. darauf, ob der Verantwortliche genehmigte Verhaltensregeln oder ein genehmigtes Zertifizierungssystem gemäß den Art. 40 und 42 der Verordnung eingehalten hat.

42. Die Einführung von Verhaltensregeln oder Zertifizierungssystemen kann ein nützliches Element der Bewertung zum Zweck der Erfüllung der Beweispflicht und der damit verbundenen gerichtlichen Überprüfung darstellen. Allerdings ist klarzustellen, dass es nicht ausreicht, dass der Verantwortliche Verhaltensregeln eingehalten hat, sondern dass er gemäß dem Grundsatz der Rechenschaftspflicht nachweisen muss, dass er die darin vorgesehenen Maßnahmen tatsächlich ergriffen hat. Die Zertifizierung hingegen stellt „als solche den Beweis für die Übereinstimmung der durchgeführten Verarbeitungen mit der Verordnung dar, auch wenn sie in der Praxis widerlegt werden kann“ [15].

43. Schließlich ist darauf hinzuweisen, dass diese Maßnahmen gemäß Art. 24 Abs. 1 erforderlichenfalls überprüft und aktualisiert werden müssen. Auch dies wird Gegenstand der vom nationalen Gericht anzustellenden Prüfung sein. Art. 32 Abs. 1 der Verordnung [16] verpflichtet den Verantwortlichen nämlich zu einer ständigen Kontrolle und Überwachung vor und nach der Verarbeitung und zur Erhaltung und eventuellen Aktualisierung der getroffenen Maßnahmen, um Verstöße zu verhindern und gegebenenfalls ihre Auswirkungen zu begrenzen.

44. Ich würde jedoch dazu neigen, die Wahrscheinlichkeit auszuschließen, dass das nächste Urteil eine Liste materieller Elemente enthalten wird, wie sie von der portugiesischen Regierung vorgeschlagen wurde [17]. Dies könnte Raum für widersprüchliche Auslegungen bieten, da die Aufzählung natürlich niemals erschöpfend sein kann.

15 M. Gambini, *Responsabilità*, oben angeführt, S. 1067. Der Besitz eines Zertifikats führt daher zu einer Umkehr der Beweislast zugunsten des Verantwortlichen, dem der Beweis erleichtert wird, im Einklang mit den sich aus der Verordnung ergebenden Verpflichtungen gehandelt zu haben.

16 Indem unter dem Buchst. d ausdrücklich bestimmt wird, dass sich die Beurteilung der Geeignetheit auf die Wirksamkeit der getroffenen Maßnahmen erstreckt, die sowohl in der Anfangsphase als auch in regelmäßigen Abständen regelmäßig überprüft, bewertet und evaluiert werden müssen, um die Wirksamkeit aller Arten von Verarbeitungen unabhängig von ihrem Risikoniveau zu gewährleisten, und indem unter Buchst. c wiederum ausdrücklich bestimmt wird, dass die getroffenen technischen und organisatorischen Maßnahmen in der Lage sein müssen, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen. Vgl. M. Gambini, *Responsabilità*, oben angeführt, S. 1064 und 1065.

17 Rn. 30 der schriftlichen Erklärungen: „Der Verantwortliche muss nachweisen, wie er alle Faktoren und Umstände im Zusammenhang mit der fraglichen Verarbeitung beurteilt hat, insbesondere das Ergebnis der durchgeführten Risikoanalyse, die ermittelten Risiken, die konkreten Maßnahmen zur Minderung dieser Risiken, die Begründung der gewählten Maßnahmen im Hinblick auf die auf dem Markt verfügbaren technischen Lösungen, die Wirksamkeit der Maßnahmen, die Wechselbeziehung zwischen den technischen und organisatorischen Maßnahmen, die Ausbildung des Personals, das die Daten verarbeitet, das Vorhandensein einer Auslagerung der Datenverarbeitungsvorgänge, einschließlich der Entwicklung und Wartung der Informationstechnologie, und das Vorhandensein einer Kontrolle durch den Verantwortlichen und konkreter Anweisungen an die Auftragsverarbeiter gemäß Art. 28 DSGVO über die Verarbeitung personenbezogener Daten durch [L]etztere; wie die Infrastruktur, die die Kommunikations- und Informationssysteme unterstützt, bewertet wurde und wie der Grad des Risikos für die Rechte und Freiheiten der betroffenen Personen eingestuft wurde“.

D. Dritte Vorlagefrage

45. Mit dem ersten Teil seiner dritten Frage möchte das vorlegende Gericht vom Gerichtshof im Wesentlichen wissen, ob unter Berücksichtigung des Grundsatzes der Rechenschaftspflicht im Sinne von Art. 5 Abs. 2 und Art. 24 in Verbindung mit dem 74. Erwägungsgrund [18] der Verordnung im Rahmen einer Schadensersatzklage nach Art. 82 der Verantwortliche nachweisen muss, dass die technischen und organisatorischen Maßnahmen im Sinne von Art. 32 geeignet sind.

46. Die vorstehenden Überlegungen erlauben mir, diese Frage zusammenfassend mit „Ja" zu beantworten.

47. Der Gesetzeswortlaut, der Zusammenhang und die Ziele der Verordnung deuten nämlich eindeutig darauf hin, dass die Beweislast bei dem Verantwortlichen liegt.

48. Aus der Formulierung verschiedener Bestimmungen der Verordnung ergibt sich, dass der Verantwortliche die Einhaltung seiner Verpflichtungen aus der Verordnung, und insbesondere, dass er zu diesem Zweck geeignete Maßnahmen ergriffen hat, „nachweisen können" muss, wie im 74. Erwägungsgrund und in Art. 5 Abs. 2 und Art. 24 Abs. 1 angegeben ist. Wie die portugiesische Regierung betont, bestimmt der 74. Erwägungsgrund, dass die dem Verantwortlichen auferlegte Beweislast auch den Nachweis der „Wirksamkeit der [fraglichen] Maßnahmen" umfassen muss.

49. Für diese wörtliche Auslegung sprechen meines Erachtens die folgenden praktischen und teleologischen Überlegungen.

50. Was die Beweislastverteilung anbelangt, so muss die betroffene Person, die Klage gegen den Verantwortlichen erhoben hat, im Rahmen einer auf Art. 82 gestützten Schadensersatzklage erstens nachweisen, dass ein Verstoß gegen die Verordnung vorliegt, zweitens, dass ihr ein Schaden entstanden ist, und drittens, dass, wie in allen schriftlichen Erklärungen zur fünften Vorlagefrage angemerkt wurde, ein kausaler Zusammenhang zwischen den beiden vorgenannten Umständen besteht. Es handelt sich dabei um drei kumulative Voraussetzungen, die sich auch aus der ständigen Rechtsprechung des Gerichtshofs und des Gerichts zur außervertraglichen Haftung der Union ergeben [19].

51. Ich bin jedoch der Auffassung, dass die Verpflichtung des Klägers, das Vorliegen eines Verstoßes gegen die Verordnung nachzuweisen, nicht so weit gehen kann, dass er nachweisen muss, dass die vom Verantwortlichen ergriffenen technischen und organisatorischen Maßnahmen im Sinne der Art. 24 und 32 nicht geeignet sind.

[18] Der 74. Erwägungsgrund lautet: „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."

[19] Vgl. insbesondere Urteile des Gerichtshofs vom 5. September 2019, Europäische Union/Guardian Europe und Guardian Europe/Europäische Union (C-447/17 P und C-479/17 P, EU:C:2019:672, Rn. 147), und vom 28. Oktober 2021, Vialto Consulting/Kommission (C-650/19 P, EU:C:2021:879, Rn. 138), sowie Urteile des Gerichts vom 13. Januar 2021, Helbert/EUIPO (T-548/18, EU:T:2021:4, Rn. 116), und vom 29. September 2021, Kočner/Europol (T-528/20, nicht veröffentlicht, EU:T:2021:631, Rn. 61), in denen darauf hingewiesen wird, dass drei Voraussetzungen vorliegen müssen, nämlich „[die] Rechtswidrigkeit des dem Unionsorgan vorgeworfenen Verhaltens, [das] tatsächliche Bestehen des Schadens und [das] Vorliegen eines Kausalzusammenhangs zwischen dem Verhalten des Organs und dem geltend gemachten Schaden".

52. Die Kommission weist darauf hin, dass die Vorlage eines solchen Nachweises in der Praxis häufig nahezu unmöglich ist, da die betroffenen Personen in der Regel weder über ausreichende Kenntnisse verfügen, um solche Maßnahmen analysieren zu können, noch Zugang zu allen Informationen haben, die sich im Besitz des Verantwortlichen befinden, insbesondere was die angewandten Methoden zur Gewährleistung der Sicherheit dieser Verarbeitung betrifft. Darüber hinaus könnte der Verantwortliche mitunter geltend machen, dass seine Weigerung, den betroffenen Personen diese Fakten mitzuteilen, auf dem legitimen Grund beruhe, seine internen Angelegenheiten oder sogar dem Berufsgeheimnis unterliegende Tatsachen, u. a. aus Sicherheitsgründen, nicht offen zu legen.

53. Würde man die Beweislast der betroffenen Person auferlegen, hätte dies in der Praxis zur Folge, dass das Recht auf einen Rechtsbehelf nach Art. 82 Abs. 1 weitgehend an Bedeutung verlieren würde. Meiner Meinung nach entspräche dies nicht den Absichten des Unionsgesetzgebers, der mit der Verabschiedung dieser Verordnung die Rechte der betroffenen Personen und die Pflichten der Verantwortlichen im Vergleich zur Richtlinie 95/46, die sie ersetzt, stärken wollte. Es ist daher logischer und rechtlich vertretbar, dass der Verantwortliche im Rahmen seiner Verteidigung gegen eine Schadensersatzklage nachweisen muss, dass er seinen Verpflichtungen aus den Art. 24 und 32 der Verordnung nachgekommen ist, indem er tatsächlich geeignete Maßnahmen getroffen hat.

54. Mit dem zweiten Teil seiner dritten Frage möchte das vorlegende Gericht vom Gerichtshof im Wesentlichen wissen, ob ein gerichtliches Sachverständigengutachten als notwendiger und ausreichender Beweis dafür betrachtet werden kann, zu beurteilen, ob die technischen und organisatorischen Maßnahmen, die der für die Verarbeitung personenbezogener Daten Verantwortliche in einer Situation getroffen hat, in der der unbefugte Zugang zu personenbezogenen Daten und deren unbefugte Offenlegung das Ergebnis eines Hackerangriffs ist, geeignet waren.

55. Ich bin der Auffassung, dass, wie auch die bulgarische und die italienische Regierung, Irland und die Kommission (im Wesentlichen) hervorgehoben haben, die Antwort auf diese Fragen sich auf unsere ständige Rechtsprechung stützen muss, wonach nach dem Grundsatz der Verfahrensautonomie in Ermangelung einschlägiger Unionsvorschriften es Sache der innerstaatlichen Rechtsordnung jedes Mitgliedstaats ist, die Verfahrensvorschriften für Gerichtsverfahren zu regeln, die dem Schutz der Rechte von Personen dienen, vorausgesetzt, dass diese Vorschriften in den durch das Unionsrecht geregelten Fällen nicht weniger günstig gestaltet sein dürfen als die Vorschriften, die für vergleichbare Fälle nach nationalem Recht gelten (Äquivalenzgrundsatz), und dass sie die Ausübung der durch das Unionsrecht verliehenen Rechte nicht praktisch unmöglich machen oder übermäßig erschweren (Effektivitätsgrundsatz).

56. Im vorliegenden Fall ist festzustellen, dass die Verordnung, insbesondere was die Ermittlungshandlungen angeht (wie etwa ein Sachverständigengutachten), die die nationalen Gerichte anordnen können oder müssen, um zu beurteilen, ob ein Verantwortlicher geeignete Maßnahmen im Sinne der Verordnung getroffen hat, keine Vorschriften zur Festlegung der zulässigen Beweismittel und ihrer Beweiskraft enthält. Daher bin ich der Auffassung, dass es in Ermangelung harmonisierter Vorschriften in diesem Gebiet Sache der innerstaatlichen Rechtsordnung der einzelnen Mitgliedstaaten ist, diese Verfahrensmodalitäten unter Beachtung der Grundsätze der Äquivalenz und der Effektivität festzulegen.

57. Der oben genannte „Effektivitätsgrundsatz“, der impliziert, dass ein unabhängiges Gericht eine unparteiische Beurteilung vornehmen muss, könnte beeinträchtigt werden, wenn das Adjektiv „ausreichend“ in dem Sinne verstanden würde, dass das vorlegende Gericht aus einem Sachverständigengutachten automatisch ableiten könnte, dass die von dem für die Verarbeitung Verantwortlichen getroffenen Maßnahmen geeignet sind [20].

E. Vierte Vorlagefrage

58. Mit der vierten Frage möchte das vorlegende Gericht im Wesentlichen wissen, ob Art. 82 Abs. 3 der Verordnung dahin auszulegen ist, dass dann, wenn ein Verstoß gegen diese Verordnung (der, wie im vorliegenden Fall in der „unbefugten Offenlegung“ oder dem „unbefugten Zugang“ zu personenbezogenen Daten im Sinne von Art. 4 Nr. 12 besteht) von Personen begangen wurde, die keine Bediensteten des Verantwortlichen sind und nicht seiner Kontrolle unterliegen, dies einen Umstand darstellt, für den der Verantwortliche in keinerlei Hinsicht verantwortlich ist, und somit ein Grund für die Befreiung von der Haftung nach Art. 82 Abs. 3 ist.

59. Die Antwort auf diese Frage ergibt sich aus den Ausführungen, die oben zu der allgemeinen Philosophie der Verordnung gemacht wurden: Es gibt keine Automatismen, und daher befreit die bloße Tatsache, dass eine unbefugte Offenlegung personenbezogener Daten oder ein unbefugter Zugang zu personenbezogenen Daten durch Personen außerhalb des Kontrollbereichs des Verantwortlichen erfolgt ist, diesen nicht von seiner Haftung.

60. Zunächst ist festzuhalten, dass weder in Art. 82 Abs. 3 noch im 146. Erwägungsgrund besondere Bedingungen festgelegt sind, die erfüllt sein müssen, damit der Verantwortliche von der Haftung befreit werden kann, mit der Ausnahme, dass er nachweisen muss, dass „er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist“. Aus dieser Formulierung ergibt sich zum einen, dass der Verantwortliche nur dann von der Haftung befreit werden kann, wenn er nachweist, dass er für den Umstand, durch den der Schaden eingetreten ist, nicht verantwortlich ist, und zum anderen, dass das von dieser Vorschrift geforderte Beweisniveau angesichts der Verwendung des Ausdrucks „in keinerlei Hinsicht“, wie von der Kommission betont wurde, hoch ist [21].

61. Über die in Art. 82 und ganz allgemein in der Verordnung vorgesehene Haftungsregelung wurde in der Lehre der verschiedenen Mitgliedstaaten viel diskutiert. Sie enthält nämlich herkömmliche Merkmale, die für die außervertragliche Haftung typisch sind, aber auch solche, die sie aufgrund des Aufbaus der Vorschriften an die vertragliche Haftung oder sogar an eine Form der Gefährdungshaftung nähern, da die Tätigkeit der Datenverarbeitung an sich schon eine

[20] Schriftliche Erklärungen, Rn. 39.

[21] Entsprechend der ständigen Rechtsprechung des Gerichtshofs, wonach Ausnahmen von einer allgemeinen Regelung restriktiv auszulegen sind, muss auch jede Haftungsbefreiung nach Art. 82 Abs. 3 restriktiv ausgelegt werden. Vgl. entsprechend Urteile vom 15. Oktober 2020, Association française des usagers de banques (C-778/18, EU:C:2020:831, Rn. 53), und vom 5. April 2022, Commissioner of An Garda Síochána u. a. (C-140/20, EU:C:2022:258, Rn. 40).

Gefahr darstellt. Hier kann nicht auf die ausführliche Debatte eingegangen werden. Allerdings scheint nach meiner Auffassung Art. 82 keine Regelung über eine Gefährdungshaftung zu enthalten [22].

62. Ein Schaden infolge einer Verletzung des Schutzes personenbezogener Daten kann als schuldhafte Folge des Versäumnisses eintreten, angemessene und in jedem Fall geeignete technische und organisatorische Maßnahmen zu ihrer Verhinderung zu ergreifen, wobei die mit der Verarbeitungstätigkeit verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen sind. Durch diese Risiken wird die Verpflichtung zur Schadensverhütung und -vermeidung verschärft und die Sorgfaltspflicht des Verantwortlichen erweitert. Deshalb sprechen die dem Verantwortlichen auferlegten Verhaltenspflichten in Verbindung mit der Bestimmung über die Verpflichtung des Schädigers, einen Entlastungsbeweis zu erbringen, für die Anerkennung einer verschärften Haftung für mutmaßliches Verschulden bei der Haftung für die unrechtmäßige Verarbeitung personenbezogener Daten gemäß Art. 82 der Verordnung [23].

63. Daraus ergibt sich, dass der Verantwortliche die Möglichkeit hat, einen Entlastungsbeweis vorzulegen (was bei der Gefährdungshaftung nicht zulässig ist). Was die Beweislast angeht, so sieht Art. 82 Abs. 3 der Verordnung eine für den Geschädigten günstige Regelung vor, die eine Form der Umkehr der Beweislast für das Verschulden des Schädigers vorsieht [24], und zwar in gänzlicher Übereinstimmung mit der oben erwähnten Beweislastumkehr hinsichtlich der Frage, ob die getroffenen Maßnahmen geeignet sind. Der Gesetzgeber zeigt damit, dass er sich der Gefahren bewusst ist, die mit der Annahme einer anderen Verteilung der Beweislast verbunden sind; würde er nämlich die Beweislast für das Verschulden des Schädigers dem Geschädigten auferlegen, so würde dies dessen Position übermäßig belasten und damit faktisch die Wirksamkeit des Entschädigungsschutzes in einem Kontext, in dem die Vorschriften mit dem Einsatz neuer Technologien zusammenhängen, beeinträchtigen. Für den Betroffenen kann es nämlich besonders schwierig sein, die Umstände, durch die der Schaden eingetreten ist, zu rekonstruieren und einen entsprechenden Zugang zu erhalten und damit das Verschulden des Verantwortlichen nachzuweisen. Der Verantwortliche befindet sich dagegen in einer besseren Position, um einen Entlastungsbeweis zu erbringen und nachzuweisen, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist [25].

64. Der Verantwortliche muss im Einklang mit dem oben beschriebenen Grundsatz der Rechenschaftspflicht auch nachweisen, dass er alles Mögliche getan hat, um die Verfügbarkeit und den Zugang zu den Daten rasch wiederherzustellen.

[22] Von einer Gefährdungshaftung spricht man immer dann, wenn der Handelnde verpflichtet ist, alle abstrakt möglichen Maßnahmen zur Schadensvermeidung zu ergreifen, unabhängig davon, ob er sie tatsächlich kannte oder ob sie finanziell vertretbar sind. Ist der Handelnde hingegen verpflichtet, Maßnahmen zu ergreifen, die ein Unternehmer in dem betreffenden Wirtschaftszweig normalerweise ergreifen kann, um die Sicherheit aufrechtzuerhalten und Schäden zu vermeiden, die sich aus der ausgeübten Tätigkeit ergeben können, so richtet sich die Zurechnung des Schadens eher nach der Haftung für bestimmtes Verschulden. M. Gambini, *Responsabilità*, oben angeführt, S. 1055.

[23] M. Gambini, *Responsabilità*, oben angeführt, S. 1059. Im ähnlichen Sinne auch die Auffassung, wonach der Nachweis, die geeigneten Maßnahmen ergriffen zu haben, nicht in der bloßen Behauptung des Höchstmaßes an erforderlicher Sorgfalt besteht, sondern im Nachweis der Tatsache, dass der Schaden von einem Dritten verursacht wurde, begleitet von Merkmalen der Unvorhersehbarkeit und Unvermeidbarkeit, die zufälligen Ereignissen und höherer Gewalt eigen sind, S. Sica, *Sub art. 82*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta, *Codice della privacy e data protection*, Giuffrè, 2021.

[24] „[W]enn *er nachweist*, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist“ (Art. 82 Abs. 3).

[25] M. Gambini, *Responsabilità*, oben angeführt, S. 1060.

65. Kann der Verantwortliche – um auf die Frage des vorlegenden Gerichts zurückzukommen – auf der Grundlage der bisherigen Ausführungen über die Art seiner Haftung, wie oben ausgeführt, von seiner Haftung befreit werden, wenn er nachweist, dass der Verstoß auf einen Umstand zurückzuführen ist, für den er in keinerlei Hinsicht verantwortlich ist, so kann er von seiner Haftung nicht allein deshalb befreit werden, weil der Umstand von einer Person außerhalb seines Kontrollbereichs herbeigeführt wurde.

66. Wird ein Verantwortlicher Opfer eines Angriffs durch Cyberkriminelle, könnte der schadensverursachende Umstand als nicht dem Verantwortlichen zurechenbar angesehen werden. Allerdings ist nicht ausgeschlossen, dass die Nachlässigkeit des Verantwortlichen die Ursache für den fraglichen Angriff war, der durch fehlende oder ungeeignete Sicherheitsmaßnahmen für personenbezogene Daten, die er zu ergreifen hat, begünstigt wurde. Dabei handelt es sich um eine auf den Einzelfall bezogene Beurteilung des Sachverhalts, die dem angerufenen nationalen Gericht unter Berücksichtigung der ihm vorgelegten Beweise obliegt.

67. Es ist auch allgemein bekannt, dass externe Angriffe auf die Systeme öffentlicher oder privater Einrichtungen, die über eine große Menge personenbezogener Daten verfügen, weitaus häufiger sind als interne Angriffe. Der Verantwortliche muss daher geeignete Maßnahmen ergreifen, um insbesondere Angriffen von außen begegnen zu können.

68. Aus teleologischer Sicht ist schließlich festzuhalten, dass die Verordnung das Ziel eines hohen Schutzniveaus verfolgt. Dazu hat der Gerichtshof bereits hervorgehoben, dass sich aus Art. 1 Abs. 2 in Verbindung mit den Erwägungsgründen 10, 11 und 13 der Verordnung ergibt, dass Organen, Einrichtungen und sonstigen Stellen der Union sowie den zuständigen Behörden der Mitgliedstaaten die Verpflichtung auferlegt wird, für die in Art. 16 AEUV und Art. 8 der Charta garantierten Rechte ein hohes Schutzniveau in Bezug auf den Schutz personenbezogener Daten zu gewährleisten[26].

69. Sollte sich der Gerichtshof für eine Auslegung entscheiden, wonach der Verantwortliche in Fällen, in denen der Verstoß gegen die Verordnung von einem Dritten begangen wurde, automatisch von der Haftung nach Art. 82 Abs. 3 befreit werden sollte, hätte eine solche Auslegung eine mit dem von dieser Vorschrift verfolgten Schutzziel unvereinbare Wirkung, da sie die Rechte der betroffenen Personen schwächen würde, weil sie die Haftung auf Fälle beschränken würde, in denen der Verstoß durch Personen begangen wird, die dem Verantwortlichen unterstellt sind und/oder seiner Kontrolle unterliegen.

F. Fünfte Vorlagefrage

70. Mit seiner fünften Frage ersucht das vorlegende Gericht den Gerichtshof im Wesentlichen um Auslegung des Begriffs „immaterieller Schaden“ im Sinne von Art. 82 der Verordnung. Insbesondere möchte es wissen, ob die Bestimmungen von Art. 82 Abs. 1 und 2 in Verbindung

[26] Vgl. in diesem Sinne Urteil vom 15. Juni 2021, Facebook Ireland u. a. (C-645/19, EU:C:2021:483, Rn. 44 und 45).

mit den Erwägungsgründen 85 und 146[27] der Verordnung dahin auszulegen sind, dass in einem Fall, in dem der Verstoß gegen diese Verordnung in einem unbefugten Zugang zu personenbezogenen Daten und einer unbefugten Offenlegung dieser Daten durch Cyberkriminelle bestand, allein die Tatsache, dass die betroffene Person einen möglichen künftigen Missbrauch ihrer personenbezogenen Daten befürchtet, einen (immateriellen) Schaden darstellen kann, der sie zum Schadensersatz berechtigt.

71. Weder Art. 82 noch die Erwägungsgründe zum Schadensersatz liefern eine eindeutige Antwort auf diese Frage. Allerdings lassen sich daraus einige nützliche Elemente für die Analyse ableiten: Der immaterielle (oder Nichtvermögens-)Schaden kann neben dem materiellen (oder Vermögens-)Schaden Gegenstand des Schadensersatzes sein; dem Verstoß gegen die Verordnung folgt nicht automatisch der Schaden, der durch den Verstoß „verursacht" wird, oder genauer gesagt, die Verletzung des Schutzes personenbezogener Daten „kann" einen physischen, materiellen oder immateriellen Schaden für natürliche Personen „nach sich ziehen"; der Begriff des Schadens sollte im Licht der Rechtsprechung des Gerichtshofs „weit" auf eine Art und Weise ausgelegt werden, die den Zielen dieser Verordnung in vollem Umfang entspricht; der Ersatz des „erlittenen" Schadens sollte „vollständig und wirksam" sein.

72. Der Wortlaut der Bestimmungen der Verordnung schließt bereits vollkommen aus, dass kraft Natur der Sache Schäden vorliegen: Das Hauptziel der von der Verordnung vorgesehenen zivilrechtlichen Haftung besteht darin, der betroffenen Person gerade durch einen „vollständigen und wirksamen" Ersatz des erlittenen Schadens Genugtuung zu verschaffen und damit das Gleichgewicht der durch die Rechtsverletzung negativ beeinflussten Rechtslage wiederherzustellen[28].

73. Andererseits sieht die Verordnung auch aus systematischer Sicht, wie im Kartellrecht, zwei Schutzpfeiler vor: einen öffentlich-rechtlichen, der Sanktionen bei Verstößen gegen die Bestimmungen der Verordnung vorsieht, und einen privatrechtlichen, der eine zivilrechtliche Haftung außervertraglicher Art vorsieht, die bei vermutetem Verschulden mit den oben genannten Merkmalen, auch im Hinblick auf den Entlastungsbeweis, als verschärft eingestuft werden kann[29].

[27] Im 85. Erwägungsgrund heißt es: „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 …"; im 146. Erwägungsgrund heißt es: „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. … Die betroffenen Personen sollten einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhalten …"

[28] Vgl. angeführte Schlussanträge des Generalanwalts Campos Sánchez-Bordona (Nr. 29 und Fn. 11). In diesen Schlussanträgen schließt der Generalanwalt seine Analyse unter wörtlichen, geschichtlichen, kontextuellen und teleologischen Gesichtspunkten korrekt ab, indem er den „Strafcharakter" des Schadensersatzes für die betroffenen Personen gemäß Art. 82 ausschließt (Nrn. 27 bis 55) und zum einen feststellt, dass die Mitgliedstaaten „nicht unter den Mechanismen zur Gewährleistung des Datenschutzes in Kapitel VIII zu wählen [brauchen] (und können es *de facto* auch nicht). Liegt ein Verstoß vor, der keinen Schaden verursacht, wird der betroffenen Person (zumindest) das Recht eingeräumt, bei einer Aufsichtsbehörde … eine Beschwerde einzureichen" und zum anderen, dass „die Aussicht, unabhängig von einem Schaden eine Entschädigung zu erhalten, wahrscheinlich zu zivilrechtlichen Streitigkeiten [anregt], mit womöglich nicht immer gerechtfertigten Ansprüchen, und könnte insoweit der Verarbeitung von Daten abträglich sein (Nrn. 54 und 55)".

[29] Verneint man einen Schadensersatz für schwache und vorübergehende Gefühle oder Emotionen im Zusammenhang mit Verstößen gegen Vorschriften über die Datenverarbeitung, wird die betroffene Person dadurch nicht völlig rechtlos gestellt (vgl. in diesem Sinne die angeführten Schlussanträge des Generalanwalts Campos Sánchez-Bordona, Nr. 115).

74. Eine „weit[e]“ Auslegung [30] des Begriffs des (Nichtvermögens-)Schadens kann daher nicht so weit gehen, anzunehmen, dass der Gesetzgeber darauf verzichtet hat, dass ein tatsächlicher „Schaden“ bestimmbar sein muss.

75. Die eigentliche Kernfrage ist, ob nach Feststellung des Vorliegens des Verstoßes und des Kausalzusammenhangs ein Schadensersatzanspruch allein aufgrund der von der betroffenen Person erlittenen Sorgen, Befürchtungen und Ängste vor einem möglichen künftigen Missbrauch personenbezogener Daten entstehen kann, wenn ein solcher Missbrauch nicht festgestellt wurde und/oder kein weiterer Schaden der betroffenen Person entstanden ist.

76. Nach ständiger Rechtsprechung des Gerichtshofs müssen die Begriffe einer unionsrechtlichen Bestimmung, die nicht ausdrücklich auf das Recht der Mitgliedstaaten verweist, in der Regel in der ganzen Union eine autonome und einheitliche Auslegung erhalten, die unter Berücksichtigung des Wortlauts dieser Bestimmung, ihres Zusammenhangs und der Ziele, die mit der Regelung, zu der sie gehört, verfolgt werden, und der Entstehungsgeschichte dieser Bestimmung gefunden werden muss [31].

77. Der Gerichtshof hat, worauf Generalanwalt Campos Sánchez-Bordona [32] hingewiesen hat, keine allgemeine Definition des Begriffs „Schaden“ entwickelt, die unterschiedslos in jedem Bereich anwendbar ist [33]. Was den immateriellen Schaden betrifft, so lässt sich aus seiner Rechtsprechung Folgendes ableiten: Ist eines der Ziele der auszulegenden Bestimmung der Schutz des Einzelnen oder eines bestimmten Personenkreises [34], muss der Begriff des Schadens weit ausgelegt werden; in Übereinstimmung mit diesem Kriterium erstreckt sich der Schadensersatz auf den immateriellen Schaden, auch wenn er in der auszulegenden Bestimmung nicht erwähnt wird [35].

78. Der Rechtsprechung des Gerichtshofs lässt sich zwar entnehmen, dass es im Unionsrecht einen Grundsatz des Ersatzes immaterieller Schäden gibt, doch stimme ich Generalanwalt Campos Sánchez-Bordona darin zu, dass aus ihr keine Regel abgeleitet werden kann, wonach *jeder* immaterielle Schaden, unabhängig von seiner Schwere, ersatzfähig ist [36].

30 146. Erwägungsgrund.

31 Vgl. Urteile vom 15. April 2021, The North of England P & I Association (C-786/19, EU:C:2021:276, Rn. 48), und vom 10. Juni 2021, KRONE – Verlag (C-65/20, EU:C:2021:471, Rn. 25).

32 Vgl. angeführte Schlussanträge des Generalanwalts Campos Sánchez-Bordona (Nr. 104).

33 Er hat auch nicht angegeben, welche Auslegungsmethode – autonome oder unter Bezugnahme auf das nationale Recht – zu bevorzugen ist: Dies hängt von dem Gegenstand der Prüfung ab. Vgl. Urteile vom 10. Mai 2001, Veedfald (C-203/99, EU:C:2001:258, Rn. 27), zu fehlerhaften Produkten, vom 6. Mai 2010, Walz (C-63/09, EU:C:2010:251, Rn. 21), zur Haftung der Luftfahrtunternehmen, und vom 10. Juni 2021, Van Ameyde España (C-923/19, EU:C:2021:475, Rn. 37 ff.), zur zivilrechtlichen Haftung für Unfälle, die sich im Zusammenhang mit der Benutzung von Kraftfahrzeugen ereignen.

34 Zum Beispiel Verbraucher oder Opfer von Verkehrsunfällen.

35 Im Bereich der Pauschalreisen vgl. Urteil vom 12. März 2002, Leitner (C-168/00, EU:C:2002:163); im Bereich der zivilrechtlichen Haftung für die Benutzung von Kraftfahrzeugen Urteile vom 24. Oktober 2013, Haasová (C-22/12, EU:C:2013:692, Rn. 47 bis 50), vom 24. Oktober 2013, Drozdovs (C-277/12, EU:C:2013:685, Rn. 40), und vom 23. Januar 2014, Petillo (C-371/12, EU:C:2014:26, Rn. 35).

36 Vgl. angeführte Schlussanträge des Generalanwalts Campos Sánchez-Bordona (Nr. 105). So hat der Gerichtshof die Vereinbarkeit eines nationalen Gesetzes, das für die Berechnung des Schadensersatzes bei immateriellen Schäden im Zusammenhang mit durch einen Unfall verursachten Körperverletzungen nach dem Ursprung des Unfalls unterscheidet, mit den unionsrechtlichen Vorschriften anerkannt, vgl. Urteil vom 23. Januar 2014, Petillo (C-371/12, EU:C:2014:26, Tenor): Das Unionsrecht steht „einer nationalen Rechtsvorschrift … [nicht entgegen], die in Bezug auf die Entschädigung für immaterielle Schäden, die auf leichte Körperverletzungen aufgrund von Straßenverkehrsunfällen zurückzuführen sind, eine Sonderregelung vorsieht, in der die Entschädigung für diese Schäden im Verhältnis zu der Entschädigung begrenzt wird, die für gleiche Schäden aufgrund anderer Ursachen als solcher Unfälle zuerkannt wird“.

79. In diesem Zusammenhang ist die Unterscheidung zwischen dem ersatzfähigen immateriellen Schaden und sonstigen *Nachteilen, die sich aus der Nichteinhaltung von Rechtsvorschriften ergeben* und die aufgrund ihrer geringen Schwere nicht unbedingt einen Anspruch auf Entschädigung begründen, von Bedeutung [37].

80. Der Gerichtshof erkennt diesen Unterschied insoweit an, als er Ärgernisse und Unannehmlichkeiten als eigenständige Schadenskategorie in den Bereichen bezeichnet, in denen er eine Entschädigung für solche als erforderlich erachtet [38].

81. Empirisch lässt sich feststellen, dass jeder Verstoß gegen eine Datenschutzvorschrift zu einer negativen Reaktion der betroffenen Person führt. Eine Entschädigung, die für das bloße Gefühl des Unwohlseins über die Nichteinhaltung des Gesetzes durch einen Dritten geschuldet wird, könnte leicht mit einer Entschädigung ohne Schaden verwechselt werden, was, wie wir gesagt haben, nicht vom Tatbestand von Art. 82 erfasst zu sein scheint.

82. Die Tatsache, dass unter Umständen wie denen des Ausgangsverfahrens der Missbrauch personenbezogener Daten nur möglich und nicht bereits eingetreten ist, reicht aus, um davon auszugehen, dass die betroffene Person einen durch den Verstoß gegen die Verordnung verursachten immateriellen Schaden erlitten haben kann, sofern die betroffene Person nachweist, dass die Befürchtung eines solchen Missbrauchs ihr tatsächlich und konkret einen realen und sicheren emotionalen Schaden zugefügt hat [39].

83. Die Grenze zwischen bloßer (nicht ersatzfähiger) Beunruhigung und echten (ersatzfähigen) immateriellen Schäden ist zweifellos unscharf. Allerdings sollten die nationalen Gerichte, deren Aufgabe es ist, diese Grenze von Fall zu Fall zu ziehen, eine sorgfältige Bewertung aller von der betroffenen Person, die eine Entschädigung beantragt, vorgelegten Elemente vornehmen. Diese muss die Tatsachen, die dazu führen können, dass ein „tatsächlich erlittener immaterieller Schaden“ infolge der Verletzung des Schutzes personenbezogener Daten anerkannt werden kann, genau und nicht nur allgemein darlegen, auch wenn er nicht eine im Voraus festgelegte Schwelle von besonderer Schwere erreicht: Entscheidend ist, dass es sich nicht um eine bloße subjektive Wahrnehmung handelt, die veränderlich ist und auch vom Charakter und von persönlichen Faktoren abhängt, sondern um die Objektivierung einer, wenn auch geringfügigen, aber nachweisbaren Beeinträchtigung der physischen oder psychischen Sphäre oder des Beziehungslebens einer Person; die Art der betroffenen personenbezogenen Daten und die

[37] Diese Unterscheidung findet man in einigen nationalen Rechtssystemen als unvermeidliche Folge des Lebens in der Gesellschaft. Kürzlich, zum Thema Datenschutz, in Italien: Tribunale di Palermo, sez. I civile (Gericht von Palermo, Erste Kammer für Zivilsachen), Urteil Nr. 5261 vom 5. Oktober 2017, und Cass. Civ., Ord. sec. VI (Kassationsgerichtshof, Italien, Sechste Kammer für Zivilsachen, Beschluss Nr. 17383/2020). In Deutschland u. a.: AG Diez, 7. November 2018 – 8 C 130/18, LG Karlsruhe, 2. August 2019 – 8 O 26/19, und AG Frankfurt am Main, 10. Juli 2020 – 385 C 155/19 (70). In Österreich: OGH 6 Ob 56/21k.

[38] Vgl. Urteil vom 23. Oktober 2012, Nelson u. a. (C-581/10 und C-629/10, EU:C:2012:657, Rn. 51), zur Unterscheidung zwischen „Schäden“ im Sinne von Art. 19 des am 28. Mai 1999 in Montreal geschlossenen Übereinkommens zur Vereinheitlichung bestimmter Vorschriften über die Beförderung im internationalen Luftverkehr und „Unannehmlichkeiten“ im Sinne der Verordnung Nr. 261/2004, die nach deren Art. 7 ersatzfähig sind, im Einklang mit dem Urteil vom 19. November 2009, Sturgeon u. a. (C-402/07 und C-432/07, EU:C:2009:716). In dieser Branche, wie auch im Bereich der Personenbeförderung im See- und Binnenschiffsverkehr, auf den sich die Verordnung Nr. 1177/2010 bezieht, hat der Gesetzgeber eine abstrakte Kategorie anerkannt, da der Faktor, der Ärgernisse verursacht, und das Wesen dieser Ärgernisse für alle Betroffenen identisch sind. Ich glaube nicht, dass eine solche Schlussfolgerung im Bereich des Datenschutzes möglich ist.

[39] Nach Ansicht Irlands sind diese Erwägungen im Zusammenhang mit der Cyberkriminalität in der Praxis besonders wichtig, denn wenn jede Person, die – auch nur geringfügig – von einem Verstoß betroffen ist, Anspruch auf Entschädigung für immaterielle Schäden hätte, hätte dies starke Auswirkungen, insbesondere auf die Verantwortlichen des öffentlichen Sektors, die mit begrenzten öffentlichen Mitteln finanziert werden und eher kollektiven Interessen, einschließlich der Verbesserung der Sicherheit personenbezogener Daten, dienen sollten (schriftliche Erklärungen, Rn. 72).

Bedeutung, die sie im Leben der betroffenen Person haben, und vielleicht auch die Wahrnehmung, die die Gesellschaft zu diesem Zeitpunkt von dieser spezifischen, mit der Datenverletzung verbundenen Beeinträchtigung hat [40].

IV. Ergebnis

84. Nach alledem schlage ich dem Gerichtshof vor, die Vorlagefragen wie folgt zu beantworten:

Die Art. 5, 24, 32 und 82 der Verordnung 2016/679 sind wie folgt auszulegen:

Das bloße Vorliegen einer „Verletzung des Schutzes personenbezogener Daten“ im Sinne von Art. 4 Nr. 12 reicht an sich nicht aus, um zu dem Schluss zu gelangen, dass die vom Verantwortlichen getroffenen technischen und organisatorischen Maßnahmen nicht „geeignet“ waren, um den Schutz der betreffenden Daten zu gewährleisten;

bei der Prüfung der Frage, ob die von dem für die Verarbeitung personenbezogener Daten Verantwortlichen getroffenen technischen und organisatorischen Maßnahmen geeignet waren, muss das angerufene nationale Gericht eine Überprüfung vornehmen, die sich auf eine konkrete Analyse sowohl des Inhalts dieser Maßnahmen als auch der Art und Weise ihrer Durchführung und ihrer praktischen Auswirkungen erstreckt;

bei einer Schadensersatzklage nach Art. 82 der Verordnung muss der Verantwortliche nachweisen, dass die von ihm gemäß Art. 32 der Verordnung ergriffenen Maßnahmen geeignet waren;

im Einklang mit dem Grundsatz der Verfahrensautonomie ist es Sache der innerstaatlichen Rechtsordnung jedes Mitgliedstaats, die zulässigen Beweismittel und deren Beweiskraft zu bestimmen, einschließlich der Ermittlungsmaßnahmen, die die nationalen Gerichte anordnen können oder müssen, um zu beurteilen, ob ein Verantwortlicher geeignete Maßnahmen im Sinne dieser Verordnung unter Beachtung der im Unionsrecht festgelegten Grundsätze der Äquivalenz und der Effektivität getroffen hat;

der Umstand, dass der Verstoß gegen diese Verordnung, der den fraglichen Schaden verursacht hat, von einem Dritten begangen wurde, stellt für sich genommen keinen Grund dar, den Verantwortlichen von der Haftung zu befreien, und der Verantwortliche muss, um in den Genuss der von dieser Bestimmung vorgesehenen Befreiung zu kommen, nachweisen, dass er für den Verstoß in keinerlei Hinsicht verantwortlich ist;

der Schaden, der in der Befürchtung eines möglichen künftigen Missbrauchs ihrer personenbezogenen Daten besteht und dessen Vorhandensein die betroffene Person nachgewiesen hat, kann einen immateriellen Schaden darstellen, der einen Schadensersatzanspruch begründet, sofern die betroffene Person nachweist, dass sie individuell einen realen und sicheren emotionalen Schaden erlitten hat, ein Umstand, den das angerufene nationale Gericht in jedem Einzelfall zu prüfen hat.

[40] Vgl. angeführte Schlussanträge des Generalanwalts Campos Sánchez-Bordona (Nr. 116).