Urteil des EuGH in der Rechtssache C-340/21 – 14.12.2023

Finanzamt Bulgarien | Natsionalna agentsia za prihodite (NAP)

Cyberkriminalität: Die Befürchtung eines möglichen Missbrauchs personenbezogener Daten kann für sich genommen einen immateriellen Schaden darstellen.

So lautet der Überschrift der Pressmitteilung Nr. 191/23 in der Rechtssache C-340/21. Das Urteil ist bereits abrufbar - CURIA - Dokumente (europa.eu). Nachfolgend haben wir für Sie die wichtigsten Punkte dieses Urteils auf Deutsch zusammengefasst.

Die Fakten: Am 15. Juli 2019 wurde in den bulgarischen Medien bekannt, dass sich Unbefugte Zugang zum Informationssystem des Finanzamts der Republik Bulgarien, der NAP, verschafft hatten. In Folge dieses Cyberangriffs wurden in diesem Informationssystem enthaltene personenbezogene Daten im Internet veröffentlicht.

Mehrere Millionen natürliche Personen, sowohl bulgarische als auch ausländische Staatsangehörige, waren von diesen Ereignissen betroffen. Mehrere Hundert von ihnen, darunter die Klägerin des Ausgangsverfahrens, erhoben gegen die NAP Klagen auf Ersatz des immateriellen Schadens, den sie infolge der Veröffentlichung ihrer personenbezogenen Daten erlitten zu haben behaupteten.

Die Klägerin im o. g. Verfahren behauptet insbesondere, dass ihr immaterieller Schaden in der Befürchtung bestand, dass ihre persönlichen Daten, die ohne ihre Zustimmung veröffentlicht worden waren, in Zukunft missbraucht werden könnten, bzw. dass sie selbst erpresst, angegriffen oder sogar entführt werden könnte.

Was behauptet die NAP?

- dass die Klägerin des Ausgangsverfahrens von ihr keine Informationen über die konkreten personenbezogenen Daten, die weitergegeben worden seien, verlangt habe.

- dass kein Kausalzusammenhang zwischen dem behaupteten immateriellen Schaden und dem Verstoß besteht.

- dass da sie selbst Ziel eines böswilligen Angriffs durch andere Personen als ihre Mitarbeiter gewesen sei und somit **nicht für die schädlichen Folgen dieses Eingriffs haftbar gemacht werden dürfe.**

In seiner Entscheidung vom 27. November 2020 wies das Verwaltungsgericht Sofia-Stadt die Klage der Klägerin im Ausgangsverfahren ab. Das Gericht stellt zum einen fest, dass der unbefugte Zugriff auf die Datenbank der NAP durch einen Hackerangriff Dritter erfolgt sei, und zum anderen, dass die Klägerin des Ausgangsverfahrens nicht nachgewiesen habe, dass die NAP es unterlassen habe, Sicherheitsmaßnahmen zu ergreifen. **Außerdem ist sie der Ansicht, dass der Klägerin kein ersatzfähiger immaterieller Schaden entstanden sei.**

Die Klägerin des Ausgangsverfahrens legte gegen diese Entscheidung Rechtsmittel beim Obersten Verwaltungsgericht in Bulgarien ein, das im vorliegenden Fall das vorlegende Gericht ist.

Zur Begründung ihres Rechtsmittels macht Oberste Verwaltungsgericht geltend:

- dass das Gericht die Beweislast für die von der NAP getroffenen Sicherheitsmaßnahmen rechtsfehlerhaft verteilt habe und

- dass die NAP nicht nachgewiesen habe, dass sie in dieser Hinsicht nicht untätig gewesen sei.

- dass die Angst vor einem möglichen künftigen Missbrauch ihrer personenbezogenen Daten **kein hypothetischer, sondern ein realer immaterieller** Schaden sei.

Die NAP bestreitet jedes dieser Argumente.

Mit seiner ersten Frage möchte das vorlegende Gericht, das Oberste Verwaltungsgericht, im Wesentlichen wissen, ob die Art. 24 und 32 DSGVO dahingehend auszulegen sind, dass die unbefugte Offenlegung personenbezogener Daten oder der unbefugte Zugang zu solchen Daten durch einen "Dritten" im Sinne von Art. 4 Nr. 10 der Verordnung allein ausreicht, um festzustellen, dass die von dem für die Verarbeitung Verantwortlichen angewandten technischen und organisatorischen Maßnahmen nicht "angemessen" im Sinne der Art. 24 und 32 DSGVO sind.

EuGH: Die Artikel 24 und 32 DSGVO können nicht so verstanden werden, dass die unbefugte Offenlegung personenbezogener Daten oder der unbefugte Zugriff auf solche Daten durch einen Dritten ausreicht, um zu dem Schluss zu kommen, dass die von dem für die Verarbeitung Verantwortlichen getroffenen Maßnahmen im Sinne dieser Bestimmungen nicht angemessen sind, ohne dass der für die Verarbeitung Verantwortliche Gegenbeweis erbringen kann (Rn. 31).

Der Verantwortliche muss in der Lage sein, die Vereinbarkeit, der von ihm getroffenen Maßnahmen mit der DSGVO, nachzuweisen, eine Möglichkeit, die ihm bei Annahme einer unwiderlegbaren Vermutung verwehrt wäre (Rn. 32).

Art. 24 und 32 DSGVO seien dahingehend auszulegen, dass eine unbefugte Offenlegung von bzw. ein unbefugter Zugang zu personenbezogenen Daten durch „Dritte“ im Sinne von Art. 4 Nr. 10 DSGVO allein nicht ausreichend ist, um anzunehmen, dass die technischen und organisatorischen Maßnahmen, die der für die betreffende Verarbeitung Verantwortliche getroffen hat, nicht „geeignet“ im Sinne der Art. 24 und 32 DSGVO waren (Rn. 39).

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

EuGH: Art. 32 DSGVO ist dahin auszulegen, dass die Beurteilung der Angemessenheit der von dem für die Verarbeitung Verantwortlichen nach diesem Artikel getroffenen technischen und organisatorischen Maßnahmen von den nationalen Gerichten im Einzelfall vorzunehmen ist, wobei die mit der betreffenden Verarbeitung verbundenen Risiken zu berücksichtigen sind und zu beurteilen ist, ob Art, Umfang und Anwendung dieser Maßnahmen in einem angemessenen Verhältnis zu diesen Risiken stehen (Rn. 47).

Mit dem ersten Teil seiner dritten Frage möchte das vorlegende Gericht im Wesentlichen wissen, ob der in Art. 5 Abs. 2 verankerte und in Art. 24 DSGVO konkretisierte Grundsatz der der Rechenschaftspflicht des für die Verarbeitung Verantwortlichen dahingehend auszulegen ist, dass in einem Schadensersatzverfahren nach Art. 82 dieser Verordnung der für die Verarbeitung **Verantwortliche die Beweislast dafür trägt**, dass die von ihm nach Art. 32 dieser Verordnung getroffenen Sicherheitsmaßnahmen **angemessen sind.**

EuGH: Der in Art. 5 Abs. 2 verankerte und in Art. 24 DSGVO konkretisierte Grundsatz der Rechenschaftspflicht des für die Verarbeitung Verantwortlichen ist dahingehend auszulegen, dass im Rahmen einer Schadensersatzklage nach Art. 82 DSGVO der für die Verarbeitung Verantwortliche die Beweislast dafür trägt, dass die von ihm nach Art. 32 DSGVO getroffenen Sicherheitsmaßnahmen angemessen sind (Rn. 57).

Mit dem zweiten Teil seiner dritten Frage möchte das vorlegende Gericht im Wesentlichen wissen, ob Art. 32 DSGVO und der unionsrechtliche Effektivitätsgrundsatz dahingehend auszulegen sind, dass zur Beurteilung der Angemessenheit der, von dem für die Verarbeitung Verantwortlichen auf der Grundlage dieses Artikels getroffenen Sicherheitsmaßnahmen, die Beauftragung eines Sachverständigengutachtens als notwendiges und ausreichendes Beweismittel angesehen werden kann.

EuGH: Die DSGVO enthält keine Regeln über die Zulassung und den Beweiswert eines Beweismittels, wie eines Sachverständigengutachtens, die von den nationalen Gerichten anzuwenden sind, die mit einer auf Art. 82 DSGVO gestützten Schadenersatzklage befasst sind und die Geeignetheit der, von dem für die betreffende Verarbeitung Verantwortlichen getroffenen Sicherheitsmaßnahmen, im Hinblick auf Art. 32 DSGVO zu beurteilen haben. In Ermangelung einschlägiger unionsrechtlicher Vorschriften ist es die Aufgabe der innerstaatlichen Rechtsordnung des einzelnen Mitgliedstaats, die Ausgestaltung von Klageverfahren, die den Schutz der dem Einzelnen aus Art. 82 DSGVO erwachsenden Rechte gewährleisten sollen, und insbesondere die Regeln für die Beweismittel, anhand deren die Geeignetheit solcher Maßnahmen in diesem Zusammenhang bewertet werden kann, festzulegen, wobei der Äquivalenz- und der Effektivitätsgrundsatz zu beachten sind (Rn. 60).

Art. 32 DSGVO und der unionsrechtliche Effektivitätsgrundsatz sind dahin auszulegen, dass für die Beurteilung der Geeignetheit der Sicherheitsmaßnahmen, die der Verantwortliche nach diesem Artikel getroffen hat, ein Sachverständigengutachten kein generell notwendiges und ausreichendes Beweismittel sein kann. (Rn. 64).

Mit seiner vierten Frage möchte das vorlegende Gericht wissen, ob Art. 82 Abs. 3 DSGVO dahingehend auszulegen ist, dass der für die Verarbeitung Verantwortliche von seiner Verpflichtung nach Art. 82 Abs. 1 und 2 dieser Verordnung, einer Person den erlittenen Schaden zu ersetzen, nur deshalb befreit ist, weil dieser Schaden auf die unbefugte Weitergabe personenbezogener Daten oder den unbefugten Zugang zu solchen Daten durch einen ,,Dritten'' im Sinne von Art. 4 Nr. 10 der DSGVO zurückzuführen ist.

EuGH: Ein für die Verarbeitung Verantwortlicher ist grundsätzlich verpflichtet, den durch einen Verstoß gegen diese Verordnung verursachten Schaden, im Zusammenhang mit dieser Verarbeitung, zu beheben. Er ist andererseits nur dann von der Haftung frei, wenn er nachweisen kann, dass er in keiner Weise für das Ereignis verantwortlich ist, das diesen Schaden verursacht hat (Rn. 69)

Im Falle einer von einem Dritten begangenen Verletzung des Schutzes personenbezogener Daten kann der für die Verarbeitung Verantwortliche auf der Grundlage von Artikel 82 Absatz 3 DSGVO von der Haftung befreit werden, wenn er nachweist, dass kein Kausalzusammenhang zwischen der möglichen Verletzung der Pflicht zum Schutz personenbezogener Daten durch den für die Verarbeitung Verantwortlichen und dem der natürlichen Person entstandenen Schaden besteht (Rn. 72)

Es erfolgt keine Befreiung von Haftung für Verantwortliche, nur weil diese Schaden auf die unbefugte Weitergabe personenbezogener Daten oder den unbefugten Zugriff zu solchen Daten durch einen ,,Dritten'' im Sinne von Art. 4 Nr. 10 der DSGVO zurückzuführen ist (Rn. 74).

Mit seiner fünften Frage möchte das vorlegende Gericht im Wesentlichen wissen, ob Art. 82 Abs. 1 DSGVO dahingehend auszulegen ist, dass die Furcht einer betroffenen Person vor einem möglichen Missbrauch ihrer personenbezogenen Daten durch einen Dritten infolge eines Verstoßes gegen diese Verordnung an sich einen ,, immateriellen Schaden'' im Sinne dieser Bestimmung darstellen kann.

EuGH: Beruft sich eine Person, die einen Rechtsbehelf aus diesem Grund einlegen will, auf die Befürchtung, dass ihre personenbezogenen Daten aufgrund einer solchen Verletzung in Zukunft missbraucht werden könnten, muss das angerufene nationale Gericht prüfen, **ob diese Befürchtungen unter Berücksichtigung der Umstände des Einzelfalls und der Person des Betroffenen als begründet angesehen werden können** (Rn. 85).

Art. 82 Abs. 1 DS-GVO ist dahin auszulegen, dass allein die Befürchtung einer betroffenen Person, dass ihre personenbezogenen Daten infolge eines Verstoßes gegen diese Verordnung von Dritten missbraucht werden könnten, für sich genommen einen "immateriellen Schaden" im Sinne dieser Bestimmung darstellen kann (Rn. 86).

Was passierte tatsächlich nach der Hackerattacke gegen die NAP?

Am 15.07.2019 wurden personenbezogene Daten von ca. 4 Millionen bulgarischen und ca. 200.000 ausländischen Staatsangehörigen unrechtmäßig veröffentlicht. Die NAP informierte auf ihrer Webseite, dass es für jeden möglich ist, zu überprüfen, ob die Sicherheit seiner persönlichen Daten durch einen unbefugten externen Zugriff auf die Daten verletzt wurde.

Welche Informationen wurden natürlichen und juristischen Personen zur Verfügung gestellt? (Quelle: НАП проверка (nra.bg)**)**

- Namen, persönliche Identifikationsnummern und Adressen von bulgarischen Staatsbürgern;
- Namen, Identifikationsnummer, Geburtsdatum, Adresse ausländischer Bürger;
- Telefone, E-Mail-Adressen;
- Steuer- und Sozialversicherungsinformationen,
- Daten aus den jährlichen Steuererklärungen von natürlichen Personen;
- Daten aus Einkommenserklärungen von natürlichen Personen;
- Daten aus Sozialversicherungserklärungen;
- Daten zum Krankenversicherungsstatus. Es handelte sich hier um Versicherungsbeiträge, nicht um Informationen über den medizinischen Status oder die Behandlung der Bürger;
- Daten über Ordnungswidrigkeiten;
- Daten über die Zahlung von Steuern und Sozialversicherungsbeiträgen durch die Bulgarische Post AG;
- Daten aus Mehrwertsteuererstattungsanträgen, die in einem anderen EU-Mitgliedstaat gezahlt wurden;
- Daten aus dem internationalen automatischen Austausch von Steuerinformationen für bulgarische und ausländische Personen;
- Offizielle Daten, die von anderen Institutionen an der NAP übermittelt wurden, wie z.B. die Zollbehörde, die Agentur für Arbeit, die Sozialhilfebehörde, die Nationale Krankenkasse der Republik Bulgarien (NHIF) u. a.

Weiter publiziert die NAP auf der Webseite das Folgende (Quelle: НАП проверка - nra.bg):

Was kann ich tun, um die NAP zur Verantwortung zu ziehen?

Schadensersatzansprüche, die sich aus illegal verbreiteten Daten ergeben, können vor Gericht geltend gemacht werden. Die NAP und die Bürger der Republik Bulgarien sind Opfer eines Verbrechens, das von den zuständigen Behörden als Terrorismus definiert wurde. Derzeit gibt es keine Beweise für eine interne Verwicklung von Mitarbeitern der NAP.

Häufig gestellten Fragen werden auch auf Englisch auf der Webseite publiziert - НАП проверка (nra.bg).

Als Ergebnis folgten Schadenersatzklagen. Offenbar wurden in erster Instanz viele Klagen abgewiesen. Einer der Hauptgründe war, dass der immaterielle Schaden, wie z. B. die Sorge und Angst vor möglichem künftigen Missbrauch, hypothetisch seien.

Die Gerichtsverfahren gegen die NAP wurden in erster Instanz mit widersprüchlichen Ergebnissen abgeschlossen. Die Klagen wurden entweder als unbegründet abgewiesen oder es wurde ihnen ganz oder teilweise stattgegeben.

Die Rechtsvorschriften wurden in Bezug auf alle Elemente der Haftung des für die Datenverarbeitung Verantwortlichen uneinheitlich ausgelegt und angewandt.

Bei dem Obersten Verwaltungsgericht als Kassationsinstanz wurden mehr als 100 Fälle eingereicht. Der Oberste Verwaltungsgericht vertrat die Auffassung, dass die NAP untätig geblieben ist, ihren Verpflichtungen aus den Artikeln 24 und 32 der DSGVO nicht nachgekommen ist und nicht nachgewiesen hat, dass sie geeignete technische Maßnahmen ergriffen hat, die ein angemessenes Sicherheitsniveau gewährleistet haben. Die negativen Emotionen, Sorgen, Ängste und Unsicherheiten der betroffenen Person stehen in kausalem Zusammenhang mit dem Verhalten des für die Verarbeitung Verantwortlichen und stellen einen echten immateriellen Schaden dar, der mit der realen Furcht vor einem tatsächlich drohenden Schaden verbunden ist. (Quelle: Върховен административен съд :: ВАС отправя преюдициално запитване до Съда на ЕС във връзка с дело срещу НАП за теча на лични данни (justice.bg).

Aufgrund widersprüchlicher Gerichtsentscheidungen hatte das bulgarische Gericht ein Ersuchen an den Europäischen Gerichtshof gerichtet. Der Antrag wird im Zusammenhang mit der Verwaltungssache Nr. 1037 aus dem Jahr 2021 des Obersten Verwaltungsgerichts der Republik Bulgarien gestellt, setzte aber in der Praxis die Verfahren in allen derartigen Fällen aus, bis zur jetzt vorliegenden Entscheidung des Europäische Gerichtshof.

Wie geht es in den ausgesetzten Verfahren weiter?

Wir werden die Entwicklung und die Entscheidungen der bulgarischen Gerichte weiterverfolgen und Sie informieren.

PRIVACY ONE ™| LEGAL

Marieta Gencheva

LL.M (Sofia), LL.M Internat. WirtschR (Halle/S.)