SG Nürnberg, Endurteil v. 10.06.2026 – S 5 SF 65/24 DS

Titel:

Hackerangriff, Verantwortlichkeit, Beweislast, Immaterieller Schaden, Feststellungsinteresse, Unterlassungsanspruch

Schlagworte:

Hackerangriff, Verantwortlichkeit, Beweislast, Immaterieller Schaden, Feststellungsinteresse, Unterlassungsanspruch

Tenor

I. Die Klage wird abgewiesen.

II. Die Klägerin hat die Kosten des Verfahrens sowie die notwendigen außergerichtlichen Kosten beider Beklagten zu tragen.

III. Der Streitwert wird auf 10.000,00 EUR festgesetzt.

Tatbestand

1
Zwischen den Beteiligten ist die Gewährung von Schadensersatz aufgrund eines geltend gemachten Datenschutzverstoßes nach einem Hackerangriff am 31.05.2023 streitig. Daneben begehrt die Klägerin die Feststellung der Schadenersatzpflicht für mögliche künftige Schäden dem Grunde nach, die Unterlassung der unbefugten Weitergabe persönlicher Daten und die Freistellung von vorgerichtlichen Rechtsanwaltskosten.

2
Die 2018 geborene Klägerin ist bei der Beklagten zu 1) gesetzlich krankenversichert und Teilnehmerin an deren Bonusprogramm, das über eine App betrieben wird. Hierbei werden für jeweils 100 gesammelte Punkte 10,00 € an den Versicherten ausbezahlt. Punkte können durch die regelmäßige Teilnahme an Vorsorgeuntersuchungen sowie Sport- und Freizeitprogrammen gesammelt werden. Für die informationstechnische Abwicklung ihres Bonusprogramms bedient sich die Beklagte zu 1) eines Auftragsverarbeiters, der Beklagten zu 2). Die Beklagte zu 2) nutzt für die Erbringung der geschuldeten Dienstleistungen das Programm M-IT des USamerikanischen Unternehmens P-Corp. (nachfolgend: „P.“). Hierbei handelt es sich um eine Software zum Austausch von Daten. Die Beklagte zu 1) hat mit der Beklagten zu 2) eine Vereinbarung über die Auftragsverarbeitung geschlossen. Die dazugehörigen allgemeinen Rahmenbedingungen „Informationssicherheit“ regeln die technischen und organisatorischen Maßnahmen, die von der Beklagten zu 2) als Auftragsverarbeiterin einzuhalten sind. Diese enthalten unter anderem Vorgaben zur Infrastruktursicherheit und zum Schutz vor Schadsoftware. So wird von der Beklagten zu 2) z.B. verlangt, dass Schadsoftware-Erkennungs- und Reparatur-Software installiert sein muss, die dem Stand der Technik entsprechen und den Abfluss von Daten des Auftraggebers zuverlässig verhindern muss.

3
Am 31.05.2023 wurde die Beklagte zu 2) neben einer Vielzahl weltweit betroffener Unternehmen und Behörden Opfer eines Hackerangriffs der Hackergruppe C., in dessen Zuge es zu einem Datenleck gekommen ist, von dem u.a. auch die Klägerin betroffen gewesen ist. Über das Hochladen einer sog. „Web-Shell“ auf den betroffenen Server der Beklagten zu 2), gelang es den Hackern, sich Zugriff auf deren System zu verschaffen und Kundendaten – so auch die der Klägerin – abzugreifen. Bei den vom Hackerangriff betroffenen Daten handelt es sich um Vorname, Name, Krankenversicherungsnummer, Prämienbetrag (der Erlös aus der erfolgreichen Teilnahme am Bonusprogramm) und Bankverbindung (IBAN). Bei der Bankverbindung handelt es sich vorliegend nicht um die der Klägerin, sondern ihrer Mutter. Gesundheitsdaten der Klägerin waren zudem nicht betroffen. Auch sind von den Servern der Beklagten zu 1) keine Daten abgeflossen. Die Taten der Gruppe C. richteten sich – soweit bekannt – nicht gegen die jeweiligen Betroffenen, sondern gegen die von dem Angriff betroffenen Unternehmen, um diese zu erpressen. Den Hackern war es gelungen, über eine unbekannte Sicherheitslücke im Programm MOVEit an

diese Daten zu gelangen. Es handelte sich um einen sog. „zeroday-exploit“, also um eine Sicherheitslücke, die dem Softwarehersteller und den Beklagten zuvor unbekannt war. Noch am 31.05.2023 gab die Firma P. eine Sicherheitswarnung heraus. Eine entsprechende Warnung unter Hinweis auf die zuvor erfolgte Warnung von P.erfolgte seitens des Bundesamtes für Sicherheit in der Informationstechnik (BSI) am 02.06.2023 (Warnung der Sicherheitsstufe 4). Einen Tag nach Bekanntwerden der Schwachstelle am 31.05.2023 stellte P. das Sicherheitspatch zur Beseitigung der Bedrohung zur Verfügung, welches seitens der Beklagten zu 2) umgehend installiert wurden. Die Beklagte zu 1) selbst wurde über die Vorgänge nach deren Vortrag am 16.06.2023 informiert und gab am nächsten Tag eine entsprechende Pressemitteilung heraus. In der Folge informierte sie auch die Eltern der Klägerin als gesetzliche Vertreter.

4
Mit anwaltlichem Schreiben vom 27.03.2024 forderte die Klägerin die Beklagte zu 1) zur Unterlassung, zur Zahlung von Schmerzensgeld in Höhe von mindestens 3.000,00 € sowie zur Verpflichtung auf, der Klägerin alle zukünftigen Schäden zu ersetzen, die ihr durch den unbefugten Zugriff Dritter auf die personenbezogenen Daten noch entstehen könnten.

5
Nachdem die Beklagte zu 1) mit Schreiben vom 03.04.2024 die Begehren der Klägerin abgelehnt hatte, hat diese – zunächst nur gegen die Beklagte zu 1) – Klage zum Sozialgericht Nürnberg erhoben. Mit Schriftsatz vom 12.12.2024 hat sie die Klage auf die Beklagte zu 2) erweitert. Sie sei Opfer eines Datenlecks bei der Beklagten zu 1) geworden, weil diese unzureichende technische Maßnahmen ergriffen habe, um personenbezogene Daten angemessen zu schützen. Die personenbezogenen Daten der Klägerin hätten daher von Unbefugten erlangt werden können. Die IT-Forensiker von K. hätten Hinweise dafür gefunden, dass den Hackern die Schwachstelle bereits seit dem Jahr 2021 bekannt gewesen sei. Seitdem hätten sie höchstwahrscheinlich experimentiert, wie sie die Lücke am besten missbrauchen können. Die MOVEit-Software falle seit Jahren immer wieder durch derartige (SQL-Injection) Schwachstellen auf, dahingehend habe sich auch der IT-Sicherheitsexperte T. auf X geäußert. Er spreche insbesondere davon, dass der Einsatz derartiger Software als „fahrlässig“ zu bewerten sei. Die Beklagte zu 1) hätte insbesondere folgende Schutzmaßnahmen treffen müssen: die Pseudonymisierung und/oder Verschlüsselung der personenbezogenen Daten sowie ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen. Wenn die Beklagte diese Schutzmaßnahmen ordnungsgemäß durchgeführt hätte, wäre es nicht zu dem Datenleck gekommen und Unbefugte hätten nicht Zugriff auf die Daten der Klägerin erhalten. Selbst wenn das Datenleck „nur“ bei der Beklagten zu 2) eingetreten wäre, so läge auch in diesem Fall eine Haftung der Beklagten zu 1) vor. Denn diese müsse als datenschutzrechtliche Verantwortliche sicherstellen, dass all ihre Vertragspartner, die im Rahmen einer Auftragsverarbeitung personenbezogene Daten von Barmer-Kunden verarbeiten, ebenfalls datenschutzkonform arbeiten. Dazu hätte die Beklagte den Auftragsverarbeiter entsprechend anleiten und überwachen müssen. Beide Beklagte seien gemeinsame Verantwortliche nach Art. 26 der Datenschutzgrundverordnung (DSGVO). Die Verwendung der MOVEit Software sei zum Zeitpunkt als das Datenleck von der Hackergruppe ausgenutzt wurde grob fahrlässig. Durch eine modernere, wenn auch teurere Software wäre das Datenleck vermieden worden. Die Beklagte zu 1) sei nach Art. 32 DSGVO verpflichtet, angemessene und geeignete technische und organisatorische Maßnahmen (TOM) zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die Beklagte zu 1) habe es pflichtwidrig versäumt, in technischer und organisatorischer Hinsicht geeignete Maßnahmen zu ergreifen und zu implementieren, um eine Offenlegung von personenbezogenen Daten zu verhindern. Die Beklagte habe daher (auch) die Vorgaben des Art. 32 DSGVO verletzt. Durch den anhaltenden Kontrollverlust über persönliche und sensible Daten stehe der Klägerin ein immaterieller Schadensersatzanspruch aus Art. 82 Abs. 1 DSGVO zu. Der tatsächliche Schaden läge in dem andauernden Zustand bestehender und belastender Ungewissheit über die unbefugte Veröffentlichung der personenbezogenen Daten. Die Klägerin habe Sorge, dass ihre Bank- und/oder Depotdaten gehackt werden. Es müsse davon ausgegangen werden, dass die Daten der Klägerin bereits im sog. „Darknet“ zum Verkauf angeboten würden. Ferner müsse damit gerechnet werden, dass die Daten der Klägerin von Kriminellen dazu verwendet wurden oder werden, um unbefugt Zugang zu Bankkonten, Online-Diensten etc. zu erhalten, um die Klägerin finanziell zu schädigen. Die Verknüpfung und nachgelagerte Veröffentlichung von personenbezogenen Daten wie jedenfalls dem Vor- und Nachnamen sowie ggf. noch weiterer Daten öffne dem Missbrauch Tür und Tor. Der Verlust der Sozialversicherungsnummer (Anmerkung: diese wurde nicht abgegriffen, siehe oben) erhöhe zudem die Gefahr eines Identitätsdiebstahls erheblich. Zudem sei aber auch bereits der Umstand, dass die Daten der

Klägerin einer unbekannten Anzahl von unberechtigten Personen zur Verfügung stehe, für sie beängstigend, da noch nicht bekannt sei, auf welche Weise diese zweckentfremdet zum Einsatz kommen können. Zudem habe die Beklagte ausgehend von einem Gegenstandswert von 10.000,00 € die vorgerichtlichen Rechtsanwaltskosten der Klägerin zu tragen.

6
Die Klägerin beantragt,

1. die Beklagten werden als Gesamtschuldner verurteilt, an die Klägerseite als Ausgleich für Datenschutzverstöße einen immateriellen Schadensersatz, dessen Höhe in das Ermessen des Gerichts gestellt wird, den Betrag von 3.000,00 € aber nicht unterschreiten sollte, nebst Zinsen in Höhe von 5%-Punkten über den jeweiligen Basiszinssatz seit Rechtshängigkeit zu zahlen.

2. Es wird festgestellt, dass die Beklagten verpflichtet sind, der Klägerseite alle materiellen künftigen Schäden zu ersetzen, die der Klägerseite durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten mit den personenbezogenen Daten der Klagepartei, der nach bisherigen Informationen am 31.05.2023 erfolgte, entstanden sind und/oder noch entstehen werden.

3. Die Beklagten werden verurteilt, es bei Meidung eines für jeden Fall, der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu € 250.000,00, ersatzweise an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft, oder einer an ihrem gesetzlichen Vertreter zu vollstreckender Ordnungshaft bis zu 6 Monaten, im Wiederholungsfall bis zu 2 Jahren, zu unterlassen, personenbezogene Daten der Klägerseite, namentlich Vorname, Name, Krankenversicherungsnummer, Prämienbetrag, sowie die Bankverbindung, Dritten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzunehmen und ohne, dass eine Einwilligung der Klägerin vorliegt oder ein Rechtfertigungsgrund nach der DSGVO.

4. Die Beklagte zu 1) wird verurteilt, die Klagepartei von den außergerichtlich entstandenen Kosten für die anwaltliche Rechtsverfolgung in Höhe von 973,65 € nebst Zinsen in Höhe von 5%-Punkten über den jeweiligen Basiszinssatz ab Rechtshängigkeit freizustellen.

7
Die Beklagten beantragen,

die Klage abzuweisen.

8
Die Beklagte zu 1) trägt vor, dass nicht bekannt sei, dass personenbezogene Daten der Klägerin irgendwo veröffentlicht worden wären. Es fehle vorliegend bereits an einer der Beklagten zurechenbaren Rechtsverletzung. Sie sei deswegen von der Haftung befreit (Art. 82 Abs. 3 DSGVO). Eine Missachtung der Verpflichtungen aus der DSGVO durch die Beklagte zu 1) sei nicht gegeben. Sie habe für die Durchführung bestimmter Verarbeitungen personenbezogener Daten im Rahmen des Betriebs ihres Bonusprogramms die Beklagte zu 1) herangezogen. Mit dieser sei eine ordnungsgemäße Vereinbarung über die Auftragsverarbeitung nach Art. 28 DSGVO abgeschlossen worden, mit der sich diese insbesondere auch zu bestimmten TOMs verpflichtete, um den Anforderungen nach Art. 32 DSGVO gerecht zu werden. Es handele sich in Art. 32 Abs. 1 DSGVO lediglich um Beispiele für Maßnahmen, die „gegebenenfalls“ ergriffen würden. Sie seien – wenn überhaupt – nur insoweit und nur in dem Umfang umzusetzen, in dem sie zur Erreichung eines angemessenen Schutzniveaus geeignet und erforderlich seien. Insbesondere treffe Art. 32 Abs. 1 DSGVO selbst keine Entscheidung darüber, wann die Maßnahmen geboten seien. Die DSGVO verlange keinen absoluten Schutz (der auch nicht möglich wäre), sondern lediglich die technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 32 Abs. 1 DSGVO). Dass ein Hackerangriff erfolgreich gewesen sei, belege in keiner Weise das Fehlen eines angemessenen Schutzniveaus. Der anderes behauptende Vortrag der Klägerin verkenne den rechtlichen Rahmen. Im Übrigen sei bereits am 02.06.2023 das System mit einem von dem Hersteller bereitgestellten Sicherheitspatch um 10.17 Uhr gesichert worden, so dass weitere Angriffe und insbesondere der Abfluss weiterer Daten hätten unterbunden werden können. Gesundheitsdaten der Klägerin seien zudem nicht betroffen gewesen. Dass die Beklagte zu 2) wie weltweit mehrere tausend andere Unternehmen auch Opfer

eines Hackerangriffs einer Gruppe augenscheinlich russischer Krimineller geworden sei, sei für die beiden Beklagten nicht vorhersehbar gewesen. Des Weiteren lasse der Vortrag der Klägerin keinen Schaden erkennen, der ersatzfähig sein könnte. Vorliegend sei es auch ausgeschlossen, auf die Befürchtung der missbräuchlichen Verwendung der Daten als immateriellen Schaden abzustellen. Denn dafür wäre es erforderlich, dass eine missbräuchliche Verwendung unter den gegebenen Umständen und im Hinblick auf die betroffene Person tatsächlich befürchtet werden kann. Dazu fehle zum einen jeder Vortrag. Zum anderen sei es auch gänzlich unwahrscheinlich. Denn seit dem Hackerangriff auf die Auftragsverarbeiterin der Beklagten zu 1) im Mai 2023 seien nach Kenntnis der Beklagten keinerlei Betroffenendaten missbräuchlich verwendet worden. Das Ziel des Angriffs sei auch erkennbar in keiner Weise die missbräuchliche Verwendung der Betroffenendaten, sondern die Erpressung der Beklagten zu 1) als Verantwortliche und der Beklagten zu 2) als Auftragsverarbeiter. Die Beklagte zu 1) sei zudem keine „gemeinsam Verantwortliche“ mit der Beklagten zu 2) nach Art. 26 DSGVO. Es läge vielmehr ein Auftragsverarbeitungsverhältnis nach Art. 28 DSGVO vor.

9
Die Beklagte zu 2) trägt vor, dass sie niemals Zugriff auf den Quellcode der MOVEitAnwendung gehabt habe. Dieser werde vom Hersteller aus Sicherheitsgründen streng vertraulich verwahrt. Sämtliche Fehlerkorrekturen müssten daher vom Hersteller bereitgestellt werden. Die kritische Schwachstelle der MOVEit-Anwendung bilde dabei keine Ausnahme. Ihre Korrektur sei nur dem Hersteller möglich gewesen. Mobilnummer und die E-Mail-Adresse der Klägerin seien gerade nicht erbeutet worden. Mit Blick auf die Kontoverbindung könne man Schäden durch Wechsel des Kontos leicht verhindern. Die MOVEit-Anwendung sei zum Zeitpunkt des Datenschutzvorfalls unter Berücksichtigung des Stands der Technik eine sichere Anwendung gewesen und habe als unüberwindbar gegolten. Die Beklagte zu 2) habe davon ausgehen dürfen, dass die Software dem Stand der Technik entsprach. Der Hersteller der Software, die Firma P., betreue die MOVEit-Anwendung aktiv und stelle regelmäßig Updates mit Fehlerkorrekturen zur Verfügung. Dies sei auch zum Zeitpunkt des Cyberangriffs der Fall gewesen. Wie der Umgang mit dem Cyberangriff zeige, sei die von P. geleistete Betreuung auch höchst professionell erfolgt. Bereits einen Tag nach dem Bekanntwerden der am 31.05.2023 ausgenutzten Schwachstelle habe P. das Sicherheitspatch zur Beseitigung der Bedrohung zur Verfügung gestellt. Auf die zahlreichen Zertifizierungen bei P. werde verwiesen. Man selbst habe auch umfassende TOMs ergriffen, die die Beklagte zu 2) im Schriftsatz vom 19.02.2025 aufzählt. Auf diesen wird Bezug genommen. Die Beklagte zu 2) trägt ferner vor, dass sie vor dem Datenleck im Jahr 2023 jedenfalls keinerlei Kenntnis von irgendwelchen kritischen Schwachstellen der eingesetzten Software gehabt habe. Bestünde eine datenschutzrechtliche Haftung der Beklagten für den Einsatz einer Software eines sorgfältig ausgewählten Softwareherstellers, allein weil sich eine Schwachstelle der Software zeigte, deren Ausnutzung durch ordnungsgemäß getroffene flankierende Sicherheitsmaßnahmen naturgemäß nicht verhindert werden kann, würde die datenschutzrechtliche Haftung zu einer reinen Gefährdungshaftung für den Einsatz von Software ausufern. Als solche sei die datenschutzrechtliche Haftung nach Artikel 82 DSGVO nicht konzipiert, da dies jegliche Exkulpation für jeden Softwarenutzer ausschließen würde. Der Klägerin stehe es frei, P. als Hersteller in Haftung zu nehmen.

10
Die Beklagte zu 1) hat mit Schriftsatz vom 17.01.2025 einen an einen anderen Versicherten gerichteten Bescheid der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum streitgegenständlichen Hackerangriff vorgelegt. Im Bescheid ist ausgeführt: „Art. 32 DSGVO verpflichtet lediglich zur Einführung eines Risikomanagementsystems, gibt aber nicht vor, dass Verantwortliche das Risiko von Datenschutzverletzungen schlechthin beseitigen müssen (…). Selbst der Umstand, dass Dritte unbefugt Zugang zu personenbezogenen Daten erhalten können, bedeutet für sich genommen nicht, dass ergriffene technischorganisatorische Maßnahmen, nicht „geeignet“ waren. (…). Ein Datenschutzverstoß seitens der BARMER liegt somit nicht vor.“

11
Im Rahmen der mündlichen Verhandlung hat die Kammer den Vater der Klägerin informatorisch befragt. Dieser hat ausgeführt, dass es sich bei dem betroffenen Konto um das Konto der Mutter der Klägerin handele. Das Konto bestehe nach wie vor, wobei mittlerweile ein zweites Girokonto angelegt wurde. Die meisten Buchungen liefen zudem mittlerweile über sein eigenes Konto. Nach seinen Ausführungen gäbe keine Hinweise darauf, dass das Konto der Mutter der Klägerin gehackt wurde. Er wisse zudem nicht, ob die

Daten im Darknet auftauchen oder dort angeboten würden. Die Klägerin selbst habe „von dem ganzen Vorgang um das Datenleck keine Kenntnis“.

12
Hinsichtlich der weiteren Einzelheiten des Sach- und Streitstandes wird auf die Gerichtsakte nebst den wechselseitigen Schriftsätzen Bezug genommen.

Entscheidungsgründe

13
Die bezüglich der Anträge Ziff. 1 und 4 zulässige Klage ist unbegründet. Soweit die Klägerin mit Ziff. 2 eine Feststellungsklage in objektiver Klagehäufung erhebt und unter Ziff. 3 ihres Klageantrages Unterlassung begehrt, sind diese Klagen bereits unzulässig.

I.) Rechtsweg

14
Der Rechtsweg zur Sozialgerichtsbarkeit ist eröffnet. Die Klägerin rügt einen Verstoß gegen die DSGVO. Für Klagen der betroffenen Person gegen einen Verantwortlichen oder einen Auftragsverarbeiter wegen eines Verstoßes gegen diese Verordnung ist nach dem expliziten Wortlaut des § 81b Abs. 1 Zehntes Buch Sozialgesetzbuch (SGB X) der Rechtsweg zu den Gerichten der Sozialgerichtsbarkeit eröffnet (vgl. zum Schadensersatz auch Bundessozialgericht – BSG – Beschluss vom 6. März 2023 – B 1 SF 1/22 R – juris).

II.) Schadensersatz

15
Soweit die Klägerin Schadensersatz wegen eines geltend gemachten immateriellen Schadens von mindestens 3.000,00 € begehrt, erweist sich die Klage als unbegründet. Nach Art. 82 Abs. 1 DSGVO hat jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Nach Art. 82 Abs. 3 DSGVO ist die Haftung ausgeschlossen, wenn der Verantwortliche oder der Auftragsverarbeiter nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. Gemäß Art. 82 Abs. 4 DSGVO haften sowohl der Verantwortliche – hier die Beklagte zu 1) gemäß Art. 4 Nr. 7 DSGVO – als auch der Auftragsverarbeiter – hier die Beklagte zu 2) gemäß Art. 4 Nr. 8 DSGVO – gesamtschuldnerisch für einen verursachten Schaden.

16
Die Voraussetzungen für einen Schadensersatzanspruch nach Art. 82 Abs. 1 DSGVO sind nicht erfüllt. Die Kammer konnte sich nicht von einem schuldhaften Verstoß der Beklagten gegen die DSGVO überzeugen. Überdies fehlt es an einem immateriellen Schaden.

17
1.) Nach Art. 5 Abs. 1 f) DSGVO müssen personenbezogene Daten 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. Dies hat der Verantwortliche (Art. 4 Nr. 7 DSGVO) – also die Beklagte zu 1) – nachzuweisen, vgl. Art. 4 Abs. 2 DSGVO. Nach Art. 24 Abs. 1 Satz 1 DSGVO setzt der Verantwortliche 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. Nach Art. 24 Abs. 2 DSGVO müssen die Maßnahmen die Anwendung geeigneter Datenschutzvorkehrungen durch den Verantwortlichen umfassen, sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht. Art. 32 Abs. 1 DSGVO sieht zudem vor, dass der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die erfolgt 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.

18
Der Europäische Gerichtshof (EuGH) legt in seinem Urteil vom 14.12.2023 – C-340/21 – juris die wesentlichen Grundsätze nieder. Insoweit heiß es (Unterstreichungen eingefügt):

„Die Bezugnahme in Art. 32 Abs. 1 und 2 DSGVO auf „ein dem Risiko angemessenes Schutzniveau“ und ein „angemessenes Schutzniveau“ zeigt, dass mit der DSGVO ein Risikomanagementsystem eingeführt und in ihr in keiner Weise behauptet wird, dass sie das Risiko von Verletzungen des Schutzes personenbezogener Daten beseitigt“ (vgl. EuGH, a.a.O., Rn. 29). Dies zugrunde gelegt geht also auch der EuGH davon aus, dass es in einer digitalen – wie auch in der analogen Welt – keinen absoluten Schutz geben kann, sondern dass ein Risikomangementsystem Sinn und Zweck des Art. 32 DSGVO ist. In der Folge führt der EuGH aus, dass sich aus dem Wortlaut der Art. 24 und 32 DSGVO ergebe, dass diese Bestimmungen dem Verantwortlichen lediglich vorschreiben, technische und organisatorische Maßnahmen zu treffen, die darauf gerichtet sind, jede Verletzung des Schutzes personenbezogener Daten so weit wie möglich zu verhindern. Die Geeignetheit solcher Maßnahmen ist konkret zu bewerten, indem geprüft wird, ob der Verantwortliche diese Maßnahmen unter Berücksichtigung der verschiedenen in den genannten Artikeln aufgeführten Kriterien und der Datenschutzbedürfnisse getroffen hat, die speziell mit der betreffenden Verarbeitung sowie den davon ausgehenden Risiken verbunden sind (vgl. EuGH, a.a.O., Rn. 30). Sodann führt der EuGH in der Folge explizit aus (Unterstreichungen eingefügt): „Folglich können die Art. 24 und 32 DSGVO nicht dahin verstanden werden, dass eine unbefugte Offenlegung von bzw. ein unbefugter Zugang zu personenbezogenen Daten durch einen Dritten für die Schlussfolgerung ausreicht, dass die von dem für die betreffende Verarbeitung Verantwortlichen ergriffenen Maßnahmen nicht im Sinne dieser Bestimmungen geeignet waren, ohne dass ihm die Möglichkeit eingeräumt wird, den Gegenbeweis zu erbringen. Eine solche Auslegung ist umso mehr geboten, als Art. 24 DSGVO ausdrücklich vorsieht, dass der Verantwortliche den Nachweis dafür erbringen können muss, dass die von ihm umgesetzten Maßnahmen im Einklang mit der DSGVO stehen; diese Möglichkeit bliebe ihm verwehrt, wenn eine unwiderlegbare Vermutung angenommen würde“, vgl. EuGH, a.a.O., Rn. 31 f.

19
Die Beweislasst dafür, dass personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit dieser Daten im Sinne von Art. 5 Abs. 1 f) und Art. 32 DSGVO gewährleisten, obliegt dem für die betreffende Verarbeitung Verantwortlichen (vgl. EuGH, a.a.O., Rn. 52). Zum Fall von Cyberkriminalität führt der EuGH (Unterstreichungen eingefügt) aus: „Wenn, (…), eine Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO von Cyberkriminellen und damit von „Dritten“ im Sinne von Art. 4 Nr. 10 DSGVO begangen wurde, kann diese Verletzung dem Verantwortlichen nur dann zugerechnet werden, wenn dieser die Verletzung unter Missachtung einer Verpflichtung aus der DSGVO, insbesondere der Verpflichtung zum Datenschutz, die ihm nach Art. 5 Abs. 1 Buchst. f, Art. 24 und Art. 32 DSGVO obliegt, ermöglicht hat. Somit kann sich der Verantwortliche bei einer Verletzung des Schutzes personenbezogener Daten durch einen Dritten auf der Grundlage von Art. 82 Abs. 3 DSGVO von seiner Haftung befreien, indem er nachweist, dass es keinen Kausalzusammenhang zwischen der etwaigen Verletzung der Verpflichtung zum Datenschutz durch ihn und dem der natürlichen Person entstandenen Schaden gibt“, vgl. EuGH, a.a.O., Rn. 71 f.

20
Demnach entlasten Hackerangriffe zwar per se nicht von der Haftung, insbesondere dann nicht, wenn der Verantwortliche oder dessen Auftragsverarbeiter unzureichende Schutzmaßnahmen getroffen haben, vgl. dazu auch in diese Richtung EuGH, a.a.O., Rn. 74. Allerdings kann der Verantwortliche nachweisen, dass er in keinerlei Hinsicht für den Umstand, durch den der betreffende Schaden eingetreten ist, verantwortlich ist.

21
Unter Berücksichtigung dieser Grundsätze konnte sich die erkennende Kammer nicht von einer Verantwortlichkeit der Beklagten überzeugen. So haben die Beklagten substantiiert und umfassend dargelegt, dass die MOVEit-Anwendung zum Zeitpunkt des streitgegenständlichen Vorfalls im Markt als eine der marktführenden Anwendungen im Bereich Managed-File-Transferoftware etabliert war. P. bzw. deren Software war entsprechend zertifiziert. Zudem legte die Beklagte zu 2) im Schriftsatz vom 19.02.2025 umfassend eigene Maßnahmen dar, insbesondere:

- Zugriff auf die MOVEit-Anwendung nur mit Authentifikation mittels eines Nutzerkontos, wobei die Anlage von Nutzerkonten in einem stringenten Prozess erfolgte, der eine Beantragung, Genehmigung und Identitätsfeststellung vorausging.

- Jeder Nutzer erhält eine eindeutige, personalisierte, nutzerbezogene Kennung.

- In der MOVEit-Anwendung erfolgt nach 5 erfolglosen Anmeldeversuchen innerhalb eines Zeitfensters von 6 Minuten eine automatische Sperrung des Nutzerkontos für 30 Minuten. Zudem sperrt die MOVEit-Transfer-Plattform die IP-Adresse eines Endgerätes, wenn von dieser Adresse wiederholte Fehlversuche innerhalb eines Zeitfensters von 5 Minuten festgestellt wurden. Die Sperrung einer IP-Adresse kann nur von der zuständigen IT-Abteilung der Beklagten zu 2) aufgehoben werden und erfordert eine vorherige Prüfung des Vorgangs.

- Umfassende Vorgaben an das festzulegende Passwort (siehe hierzu detailliert Schriftsatz vom 19.02.2025).

- Eine Kommunikation mit der MOVEit-Transfer-Plattform ist nur über gesicherte Protokolle gestattet (FTPS, SFTP, HTTPS, Asx). Während der Dateiübertragung verwendet MOVEit SSL oder SSH zur Verschlüsselung der Kommunikation.

- Zum Zeitpunkt des Angriffs kam die Version 2021.1 (13.1.0.39) zum Einsatz und entsprach den damaligen Sicherheitsvorgaben des Herstellers.

22
Auf die weiteren aufgezeigten Maßnahmen im Schriftsatz vom 19.02.2025 wird Bezug genommen. Allein der Umstand, dass ein Hackerangriff erfolgreich gewesen ist, belegt nicht, dass die technischen und organisatorischen Maßnahmen im Vorfeld unzureichend gewesen sind (vgl. dazu Oberlandesgericht Stuttgart, Urteil vom 31.03.2021 – 9 U 34/21 – juris Rn. 54), zumal die Hacker nach dem Vortrag der Klägerin seit ca. 2021 versucht hätten, in das System einzudringen. Mithin brauchten sie – die Richtigkeit unterstellt – ca. zwei Jahre, um in das System zu kommen. Gerade die zeitliche Dauer bis zu einem erfolgreichen Angriff Ende Mai 2023 belegt auch die Sicherheit der Software. Soweit die Klägerin darauf abstellt, dass die Beklagten weitere technische Maßnahmen hätten ergreifen können, wovon sie einige aufzählt, ergibt sich hieraus keine Umsetzungspflicht, deren Nichteinhaltung einen datenschutzrechtlichen Verstoß begründen kann. Die Beklagten sind lediglich dazu verpflichtet, geeignete Maßnahmen zu treffen, die darauf gerichtet sich, eine Datenschutzverletzung so weit wie möglich zu verhindern (vgl. Landgericht Krefeld, Urteil vom 06.11.2025 – 3 O 93/24 –, juris, Rn. 30, m.w.N.). Die Auffassung des Landgerichts Krefeld zum streitgegenständlichen Hacker-Angriff vertritt auch die Kammer uneingeschränkt. So führt es aus: „Unzureichend wären die von den Beklagten beschriebenen TOM nur dann, wenn sich zuvor konkrete Anhaltspunkte für die Fehleranfälligkeit der – zum Zeitpunkt des Vorfalls – marktführenden G.-Anwendung ergeben hätten. Die Klägerin behauptet insoweit pauschal und ohne nähere Darlegung. Sie verweist hierzu auf einen unergiebigen öffentlichen Beitrag sowie auf sog. CVE-Einträge einer Fehlerdatenbank. Daraus ergibt sich indes nicht, ob die Beklagten diese Umstände vor dem Cyberangriff konkret wahrgenommen haben oder hätten wahrnehmen müssen, da insbesondere die letztgenannte Quelle vielmehr dafür spricht, dass das Programm seitens des Herstellers regelmäßig überprüft und sicherheitstechnisch weiterentwickelt wurde und wird. Gegen die Annahme, dass die Beklagten entsprechende Bedenken hätten haben müssen, spricht der Umstand, dass weltweit ca. 2.500 Unternehmen und Institutionen dem – insoweit unvorhergesehenen – sog. „zeroday-exploit“ zum Opfer fielen. Die Beklagte zu 1) hatte keinen Anlass zur verstärkten Kontrolle der Beklagten zu 2), Zweifel an der Eignung der Beklagten zu 2) als Auftragsverarbeiterin wurden nicht vorgetragen.“, vgl. Landgericht Krefeld, a.a.O., Rn. 30. Auch insoweit ist für die erkennende Kammer nicht ersichtlich, wie die Beklagten – sondern wenn überhaupt der Hersteller „P.“ – die Lücke in der Software hätten erkennen können. Das Landgericht Trier führt zudem aus: „Weiterhin war für den Datenabfluss eine Software verantwortlich, die weder von der Beklagten noch von ihrer Streithelferin entwickelt wurde, sondern von P.. Die Software war bis zum streitgegenständlichen Vorfall (unstreitig) als eine marktführende Anwendung als datensicherheits- und -schutzkonforme Austauschplattform im Markt etabliert, was sich auch in der potentiellen Betroffenheit von ca. 2.500 Unternehmen und öffentlichen Stellen durch den Cyberangriff zeigte.“, vgl. Landgericht Trier, Urteil vom 04.04.2025 – 2 O 85/24 – juris, Rn. 53. Wenn überhaupt kann daher dem Hersteller, aber nicht den Beklagten, die vollumfänglich auf die Software eines weltweiten Marktführers vertrauten, ein Vorwurf

fahrlässigen Handelns gemacht werden. Auch lässt sich zu Lasten der Beklagten zu 1) kein schuldhafter Fehler bei der Auswahlentscheidung durch die Beklagte zu 2) als Auftragsverarbeiterin feststellen.

23
Nach alledem liegt seitens der Beklagten kein (zu vertretender) Verstoß gegen die DSGVO vor.

24
2.) Überdies fehlt es im vorliegenden Fall an einem ersatzfähigen immateriellen Schaden. Die Klägerin lässt diesbezüglich schriftsätzlich vortragen, dass der tatsächliche Schaden in dem andauernden Zustand bestehender und belastender Ungewissheit über die unbefugte Veröffentlichung der personenbezogenen Daten läge. Die Umstände hätten zudem zu Sorgen und Ängsten bei der Klagepartei geführt. Die Klägerin habe zudem Sorge, dass ihre Bank und/oder Depotdaten gehackt werden. Es müsse davon ausgegangen werden, dass die Daten der Klägerin bereits im sog. „Darknet“ zum Verkauf angeboten würden. Ferner müsse damit gerechnet werden, dass die Daten der Klägerin von Kriminellen dazu verwendet wurden oder werden, um unbefugt Zugang zu Bankkonten, Online-Diensten etc. zu erhalten, um die Klägerin finanziell zu schädigen. Die Verknüpfung und nachgelagerte Veröffentlichung von personenbezogenen Daten wie jedenfalls dem Vor- und Nachnamen sowie ggf. noch weiterer Daten öffne dem Missbrauch Tür und Tor. Der Verlust der Sozialversicherungsnummer (Anmerkung: diese wurde nicht abgegriffen, siehe oben) erhöhe zudem die Gefahr eines Identitätsdiebstahls erheblich. Zudem sei aber auch bereits der Umstand, dass die Daten der Klägerin einer unbekannten Anzahl von unberechtigten Personen zur Verfügung stehe, für sie beängstigend, da noch nicht bekannt sei, auf welcher Weise diese zweckentfremdet zum Einsatz kommen können.

25
Der Vortrag der Klägerin zum behaupteten Schaden ist weitgehend unschlüssig. Zwar ist der Ersatz eines immateriellen Schadens nicht davon abhängig, dass eine bestimmte Erheblichkeitsschwelle überschritten wird (vgl. dazu EuGH, Urteil vom 04.05.2023 – C-300/21 – juris) und es kann auch nach dem Erwägungsgrund 85 DSGVO eine Verletzung des Schutzes personenbezogener Daten einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen, zum Beispiel bei Verlust der Kontrolle über personenbezogenen Daten oder Identitätsdiebstahl. Abgesehen davon, dass der Kontrollverlust aber lediglich einen Schaden darstellen kann, nicht muss, gilt es auch hier zu beachten, dass stets im zur Entscheidung stehenden Einzelfall eine entsprechende Prüfung des Vorliegens eines Schadens zu erfolgen hat. So führt der EuGH im Urteil vom 14.12.2023, a.a.O., Rn. 84 f. aus: „Allerdings ist darauf hinzuweisen, dass eine Person, die von einem Verstoß gegen die DSGVO betroffen ist, der für sie negative Folgen gehabt hat, nachweisen muss, dass diese Folgen einen immateriellen Schaden im Sinne von Art. 82 DSGVO darstellen (…). Insbesondere muss das angerufene nationale Gericht, wenn sich eine Person, die auf dieser Grundlage Schadenersatz fordert, auf die Befürchtung beruft, dass ihre personenbezogenen Daten in Zukunft aufgrund eines solchen Verstoßes missbräuchlich verwendet werden, prüfen, ob diese Befürchtung unter den gegebenen besonderen Umständen und im Hinblick auf die betroffene Person als begründet angesehen werden kann.“

26
Dementsprechend obliegt es der Kammer zu prüfen, ob die Befürchtungen der Klägerin als begründet angesehen werden können. Diesbezüglich gilt es zu beachten, dass die derzeit 8- jährige und zum Zeitpunkt des Hackerangriffs 5-jährige Klägerin nach den Ausführungen ihres Vaters im Rahmen der mündlichen Verhandlung keinerlei Kenntnis von den Vorgängen um den Verlust ihrer Daten hat. Der Vortrag in den klägerischen Schriftsätzen, wonach „belastende Ungewissheit“ über die unbefugte Veröffentlichung oder Ängste und Sorgen bestünde, erweist sich daher mangels Kenntnis der Klägerin von den Vorgängen als völlig unsubstantiiert. Wenn und soweit ausgeführt wird, dass die Klägerin Sorge habe, dass ihre Bankdaten gehackt würden, so gilt es zu beachten, dass nicht ihr Konto betroffen war, sondern das ihrer Mutter. Insoweit fragt sich, warum die Klägerin sodann – abgesehen von der fehlenden Kenntnis – Ängste haben will, wenn nicht einmal ihr Konto selbst betroffen ist. Im Übrigen bestehen keinerlei Anhaltspunkte dafür, dass die Daten im Darknet oder sonst missbräuchlich verwendet würden, zumal der Hackerangriff darauf abzielte, die betroffenen Unternehmen zu erpressen.

27
Dem steht auch nicht die Entscheidung des Bundesgerichtshofes (BGH) vom 18.11.2024 – VI ZR 10/24 – juris entgegen. Denn auch nach diesem Urteil ist eine „begründete Befürchtung“ der betroffenen Person

erforderlich und diese Befürchtung muss, samt ihrer negativen Folgen „ordnungsgemäß nachgewiesen sein“ (vgl. nach juris Rn. 32). Der BGH führt auch aus, dass die „bloße Behauptung einer Befürchtung ohne nachgewiesene negative Folgen“ ebenso wenig ausreicht, wie ein „rein hypothetisches Risiko der missbräuchlichen Verwendung durch einen unbefugten Dritten“ (vgl. nach juris Rn. 32). Dies zugrunde gelegt kann auch unter Berücksichtigung dieser Entscheidung des BGH vorliegend kein Schaden entstanden sein, nachdem hier schriftsätzlich Behauptungen zu vermeintlichen Ängsten der Klägerin aufgestellt werden, die diese mangels Kenntnis vom Datenverlust denknotwendig nicht haben kann. Es bestehen zudem nach über drei Jahren seit dem Hackerangriff nicht die geringsten Anhaltspunkte dafür, dass die Daten der Klägerin missbräuchlich verwendet wurden. Gerade das rein hypothetische Risiko einer missbräuchlichen Verwendung ist nach der Rechtsprechung des BGH nicht ausreichend, um einen immateriellen Schaden zu begründen.

28
Nach alledem fehlt es daher auch an einem ersatzfähigen Schaden. Die Klage erweist sich insoweit als unbegründet.

III.) Feststellung künftiger Schäden

29
Soweit die Klägerin festgestellt haben will, dass die Beklagten verpflichtet sind, ihr alle materiellen künftigen Schäden zu ersetzen, fehlt es bereits am Feststellungsinteresse im Sinne des § 55 Abs. 1 Sozialgerichtsgesetz (SGG). Ein Interesse an der Feststellung einer Ersatzpflicht für künftige Schäden rein materieller Art hängt von der Wahrscheinlichkeit des ausstehenden Schadenseintritts ab. Ist hingegen bei verständiger Würdigung des Einzelfalls nicht mit dem Eintritt eines künftigen Schadens zu rechnen, so ist bereits eine derartige Möglichkeit zu verneinen, vgl. Landgericht Krefeld, a.a.O., Rn. 36 m.w.N.

30
Vorliegend sind keine Umstände ersichtlich, die den Eintritt künftiger Schäden über eine bloß theoretische Befürchtung hinaus wahrscheinlich werden lassen. Abgesehen davon, dass nicht die Kontodaten der Klägerin (sondern der Mutter) betroffen waren mit der Folge, dass der Klägerin kein Schaden materieller Art entstehen kann, gilt es zu beachten, dass die Sicherheitslücke unmittelbar nach dem Hackerangriff behoben wurde. Seither kam es zu keinen Schäden materieller Art. Dabei verringert sich eine solche Möglichkeit stetig mit fortschreitendem Zeitablauf (Landgericht Krefeld, a.a.O., Rn. 36 m.w.N.). Es handelt sich daher um eine bloße theoretische Befürchtung, die ein Feststellungsinteresse nicht zu begründen vermag.

IV.) Unterlassung

31
Soweit die Klägerin Unterlassung begehrt, erweist sich die Klage als unzulässig. Die Klägerin beantragt – ähnlich wie der Kläger im Verfahren vor dem Landgericht Trier, a.a.O. – es zu unterlassen, „personenbezogene Daten der Klägerseite (…) Dritten zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzunehmen und ohne, dass eine Einwilligung der Klägerin vorliegt oder ein Rechtfertigungsgrund nach der DSGVO.“

32
Der Antrag ist zu unbestimmt. So wird nicht klar, welche Fälle des „Dritten zugänglich machens“ erfasst sein sollen und welche Sicherheitsmaßnahmen „dem Stand der Technik“ in der Zukunft entsprechen. Die erkennende Kammer schließt sich insoweit den zutreffenden rechtlichen Ausführungen des Landgerichts Trier, a.a.O., Rn. 34 ff. nach eigener Prüfung an und nimmt auf diese Bezug.

V.) Rechtsanwaltskosten

33
Mangels Bestehen eines Anspruchs nach den Klageanträgen Ziff. 1) bis 3) besteht auch kein Anspruch auf Freistellung von vorgerichtlichen Rechtsanwaltskosten.

34
Nach alledem ist die Klage daher abzuweisen.

35

Die Kostenentscheidung beruht auf § 197a Abs. 1 SG) i.V.m. § 154 Abs. 1 Verwaltungsgerichtsordnung (VwGO). Die Klägerin ist insbesondere nicht in ihrer Eigenschaft als Leistungsempfängerin nach § 183 SGG am Verfahren beteiligt und Schadensersatz bzw. die in diesem Zusammenhang geltend gemachten Feststellungs- und Unterlassungsanträge stellen keine Leistung im Sinne des § 183 SGG dar (vgl. zum Ganzen: BSG, Urteil vom 24.09.2024 – B 7 AS 15/23 R – juris m.w.N.).

36
Die Festsetzung des Streitwerts beruht auf § 197a Abs. 1 Satz 1 Halbsatz 1 SGG i.V.m. § 52 Abs. 1 und 3 Gerichtskostengesetz (GKG). Der Streitwert setzt sich zusammen aus der Hauptforderung von 3.000,00 €. Hinzu kommen die mit einem ähnlichen Wert entsprechend der Bedeutung für die Klägerin jeweils zu bemessenden Feststellungs- und Unterlassungsanträge und die beantragten vorgerichtlichen bezifferbaren Rechtsanwaltskosten, so dass sich gerundet ein Streitwert von 10.000,00 € ergibt.