Landgericht Köln, 14 O 472/23

Datum:	07.01.2025
Gericht:	Landgericht Köln
Spruchkörper:	14. Zivilkammer
Entscheidungsart:	Urteil
Aktenzeichen:	14 O 472/23
ECLI:	ECLI:DE:LGK:2025:0107.14O472.23.00

Tenor:

1. Die Beklagte wird verurteilt, an die Klägerin einen immateriellen Schadensersatz in Höhe von 100,00 € nebst Zinsen in Höhe von 5%-Punkten über dem Basiszinssatz seit dem 31.01.2024 zu zahlen.

2. Es wird festgestellt, dass die Beklagte verpflichtet ist, der Klägerin alle künftigen materiellen und immateriellen Schäden (letztere soweit sie nicht von Tenorziffer zu 1. erfasst sind) zu ersetzen, die ihr entstehen werden durch die unbefugte Veröffentlichung ihrer personenbezogenen Daten im Internet, die aufgrund eines Verschuldens der Beklagten und im Zeitraum zwischen 2019 und 2022 erfolgte.

3. Die Beklagte wird weiter verurteilt, an die Klägerin vorgerichtliche Rechtsanwaltskosten in Höhe von 220,27 € nebst Zinsen in Höhe von 5%-Punkten über dem Basiszinssatz seit dem 31.01.2024 zu zahlen.

4. Im Übrigen wird die Klage abgewiesen.

5. Die Kosten des Rechtsstreits trägt die Klägerin.

6. Das Urteil ist vorläufig vollstreckbar. Beide Parteien können die Zwangsvollstreckung durch Sicherheitsleistung i.H.v. 110% des aufgrund des Urteils vollstreckbaren Betrags abwenden, wenn nicht die jeweils andere Partei vor der Zwangsvollstreckung Sicherheit i.H.v. 110% des zu vollstreckenden Betrags leistet.

Tatbestand:

Die Parteien streiten um Ansprüche nach einem Datenschutzvorfall. 2

Die Beklagte betreibt einen Online Musikstreamingdienst unter der Internetadresse www.entfernt mit derzeit ca. 16 Millionen aktiven Nutzer. Die Beklagte ist in mehr als 180 Ländern verfügbar. Neben Musik haben Nutzer der Plattform auch Zugriff auf Hörbücher, Hörspiele und Podcasts. Nutzer können über ihren PC oder Mobiltelefon mittels der „R.“-Musikstreaming-App aus einem Online-Katalog derzeit über 90 Millionen Musikstücke, Podcasts, Hörbücher und Radiosender auf ihr Gerät streamen. 3

Die Klägerin meldete sich bei der Beklagten an. Die Beklagte speicherte über den Kläger folgende Stammdaten: 4

„Tabelle wurde entfernt“ 5

Darüber hinaus verfügt die Beklagte über Informationen, ob die Klagepartei den R.-Dienst kostenlos oder kostenpflichtig nutzte, bezüglich der Akquise-Herkunft, Hörvorlieben (angehörte Songs, Lieblingssongs, Playlists etc.) und Kommunikationspräferenzen (E-Mail-Benachrichtigungen, SMS etc.) sowie allgemeine Vertragsinformationen. 6

Die Beklagte unterhielt bis Ende 2020 vertragliche Beziehungen zu dem externen Dienstleister für Kundenverwaltungsdienste V. O. Ltd., welche wiederum Muttergesellschaft der weiteren Firma P., Inc. mit Sitz in B. war. Letztere war der operative Anbieter der von der Beklagten genutzten Dienste. Dabei bestand zwischen der Beklagten und der V. O. Ltd eine Auftragsverarbeitungsvereinbarung (Anlage B2a). Bestandteil der Vereinbarung waren Abreden zu bei der V. O. Ltd vorzuhaltenden technischen und organisatorischen Maßnahmen zum Schutz der dieser anvertrauten Daten. 7

Im Hinblick auf die Verarbeitung der Daten durch weitere Unterauftragnehmer regelt Ziff. 5 der Vereinbarung folgendes: 8

„5.1 Das Unternehmen ermächtigt den Anbieter hiermit, die in Anlage 4 aufgeführten Unterauftragsverarbeiter zu ernennen (und gestattet jedem dieser Unterauftragsverarbeiter, nach vorheriger schriftlicher Mitteilung an das Unternehmen gemäß Abschnitt 5.2 Unterauftragsverarbeiter zu ernennen), sofern die Unterauftragsverarbeiter die in Abschnitt 5.3 genannten Verpflichtungen einhalten. 9

5.2 Der Anbieter muss dem Unternehmen vorher schriftlich die Ernennung eines neuen Unterauftragsverarbeiters, einschließlich aller Einzelheiten der vom Unterauftragsverarbeiter vorzunehmenden Verarbeitung, mitteilen. Teilt das Unternehmen dem Anbieter innerhalb von zehn (10) Arbeitstagen nach Erhalt dieser Mitteilung schriftlich seine (begründeten) Einwände gegen die vorgeschlagene Ernennung mit, darf der Anbieter den vorgeschlagenen Unterauftragsverarbeiter nicht ernennen (und keine Personenbezogenen Daten des Unternehmens an ihn weitergeben), außer bei vorheriger schriftlicher Zustimmung des Unternehmens. 10

5.3 In Bezug auf jeden Unterauftragsverarbeiter verpflichtet sich der Anbieter: 11

(a) vor der ersten Verarbeitung Personenbezogener Daten des Unternehmens durch den Unterauftragsverarbeiter (oder gegebenenfalls in Übereinstimmung mit Abschnitt Erreur ! Source du renvoi introuvable.) eine angemessene DueDiligence-Prüfung durchzuführen, um sicherzustellen, dass der Unterauftragsverarbeiter in der Lage ist, das in der 12

Hauptvereinbarung geforderte Schutzniveau für die Personenbezogenen Daten des Unternehmens zu gewährleisten;

(b) sicherzustellen, dass die Vereinbarung zwischen dem Anbieter oder dem entsprechenden Unterauftragsverarbeiter einerseits und dem Unterauftragsverarbeiter andererseits durch einen schriftlichen Vertrag geregeltwird, der dieselben Datenschutzverpflichtungen enthält, wie sie in diesem Nachtrag dargelegt sind, und die Einhaltung der Anforderungen von Artikel 28 Absätze 2 bis 4 der DSGVO gewährleistet. Kommt der Unterauftragsverarbeiter seinen Datenschutzverpflichtungen nicht nach, bleibt der Anbieter dem Unternehmen gegenüber in vollem Umfang für die Erfüllung der Verpflichtungen dieses Unterauftragsverarbeiters haftbar; 13

(c) wenn diese Vereinbarung eine Übermittlung in ein Drittland beinhaltet (mit Ausnahme von Übermittlungen in die Vereinigten Staaten an einen Unterauftragsverarbeiter, der nachweislich den Anforderungen des EU-USDatenschutzschilds entspricht und unter diesem registriert ist), das Unternehmen darüber zu informieren und sicherzustellen, dass (i) angemessene Schutzmaßnahmen gemäß den Artikeln 46 und 47 der DSGVO durchgesetzt werden oder (ii) die Übermittlung in ein Drittland unter eine der in Artikel 49 der DSGVO genannten Ausnahmeregelungen fällt, und sicherzustellen, dass das Unternehmen einer solchen Analyse zustimmt. Für den Fall, dass sich die Parteien nicht über die Mittel zur Gewährleistung des Schutzniveaus der übermittelten Personenbezogenen Daten einigen, stellt der Anbieter sicher, dass die Standardvertragsklauseln zu allen relevanten Zeitpunkten in die Vereinbarung zwischen dem Anbieter oder dem jeweiligen Unterauftragsverarbeiter einerseits; und dem Unterauftragsverarbeiter andererseits, oder bevor der Unterauftragsverarbeiter zum ersten Mal Personenbezogene Daten des Unternehmens verarbeitet, dafür zu sorgen, dass er einen Vertrag mit dem Unternehmen abschließt, der die Standardvertragsklauseln enthält; und 14

(d) dem Unternehmen Kopien der mit den Unterauftragsverarbeitern geschlossenen Vereinbarungen (die zur Entfernung vertraulicher Geschäftsinformationen, die für die Anforderungen dieses Nachtrags nicht relevant sind, geschwärzt werden können) zur Überprüfung vorzulegen, die vom Unternehmen von Zeit zu Zeit angeforderten werden. 15

(…) 16

9. BEENDIGUNG DER VERARBEITUNG 17

9.1 Vorbehaltlich des Abschnitts 9.2, ist der Anbieter verpflichtet, nach Wahl des Unternehmens entweder (a) eine vollständige Kopie aller Personenbezogenen Daten des Unternehmens durch sichere Dateiübertragung in einem Format, das das Unternehmen dem Anbieter in angemessener Weise mitteilt, an das Unternehmen zurückzusenden und anschließend alle anderen Kopien der Personenbezogenen Daten des Unternehmens, die vom Anbieter oder den Unterauftragsverarbeitern verarbeitet wurden, innerhalb von einundzwanzig (21) Kalendertagen nach dem Datum der Beendigung der Dienstleistungen, die die Verarbeitung Personenbezogener Daten des Unternehmens beinhalten (das „Beendigungsdatum“), zu löschen und für die Löschung zu sorgen oder (b) die Daten innerhalb von einundzwanzig (21) Kalendertagen nach dem Beendigungsdatum zu löschen und für die Löschung aller anderen Kopien der Personenbezogenen Daten des Unternehmens, die vom Anbieter oder den Unterauftragsverarbeitern verarbeitet wurden, zu sorgen. 18

19

9.2 Der Anbieter und jeder Unterauftragsverarbeiter dürfen Personenbezogene Daten des Unternehmens nur in dem Umfang und für den Zeitraum aufbewahren, wie es die anwendbaren EU-Gesetze vorschreiben, und immer nur unter der Voraussetzung, dass der Anbieter die Vertraulichkeit aller Personenbezogenen Daten des Unternehmens sicherstellt und gewährleistet, dass diese Personenbezogenen Daten des Unternehmens nur für Zwecke verarbeitet werden, die mit denen vereinbar sind, für die sie gemäß Artikel 5.1 (b) der DSGVO erhoben wurden, und wie es die anwendbaren EU-Gesetze vorschreiben, die ihre Speicherung vorschreiben.

9.3 Der Anbieter muss dem Unternehmen schriftlich bestätigen, dass er und jeder Unterauftragsverarbeiter diesen Abschnitt 9 innerhalb von einundzwanzig (21) Kalendertagen nach dem Beendigungsdatum vollständig eingehalten haben. 20

10. INFORMATIONS- UND PRÜFUNGSRECHTE 21

10.1 Vorbehaltlich einer angemessenen schriftlichen Vorankündigung stellt der Auftragsverarbeiter dem Verantwortlichen alle erforderlichen Informationen zur Verfügung und gestattet Prüfungen, einschließlich Inspektionen, die vom Verantwortlichen oder einem anderen von ihm beauftragten Prüfer durchgeführt werden, soweit dies vernünftigerweise erforderlich ist, und leistet seinen Beitrag, um: 22

(i) zu überprüfen, ob der Auftragsverarbeiter (oder ein Unterauftragsverarbeiter) seinen Verpflichtungen gemäß Artikel 28 der DSGVO sowie den Bestimmungen dieses Nachtrags nachkommt; 23

(ii) alle Anfragen von Regulierungs- oder Aufsichtsbehörden zu erfüllen; 24

(iii) interne Audits der Datensicherheit durchführen; 25

(iv) die Integrität, Vertraulichkeit und/oder Sicherheit der Personenbezogenen Daten zu überprüfen.“ 26

Hinsichtlich der weiteren Einzelheiten wird Bezug genommen auf die Auftragsverarbeitungsvereinbarung, welche als Anlage B2a vorliegt. 27

Im Zuge der Zusammenarbeit mit den vorgenannten Firmen übermittelte die Beklagte 2019 umfangreiche Kundendaten auch an die P. Inc.. Am 30.11.2020 schrieb P. Inc. der Beklagten (im Zuge einer beklagtenseits behaupteten Beendigung des Vertragverhältnisses), dass dort sämtliche Daten der Beklagten am 1. Dezember 2020 gelöscht werden würden. In der entsprechenden Email vom 30.11.2020 heißt es: *„I wanted to notify you that as our contract terminates today, we will be deleting your site and all the data on the site tomorrow. Please confirm receipt of this email.“* (Anlage B4). 28

Zu einem zwischen den Parteien umstrittenen Zeitpunkt kam es bei P. Inc. zu einem erfolgreichen Datenzugriff unbefugter Dritter, bei dem von den Tätern ein zuvor von der Beklagten an P. Inc. übermittelter Kundendatensatz der Beklagten aus dem Jahr 2019 erlangt werden konnte. Grundsätzlich von dem Vorfall betroffen waren jedenfalls folgende Informationen einer großen Zahl von Nutzern des Dienstes der Klägerin: Vor- und Nachname, Nutzernamen, Geburtsdatum, E-Mail-Adresse, Daten über die Nutzung des D.-Dienstes, Geschlecht, Sprache, Land. Betroffen war jeweils auch die UserID, d.h. eine von der Beklagten vergebene Zahlenreihenfolge, welche einzelnen Nutzern individuell zugeordnet wird. 29

Im November 2022 wurde in den Medien darüber berichtet, dass unbekannte Hacker Daten von Nutzern der Beklagten im Dark Web zum Kauf anbieten würden. Die Beklagte veröffentlichte auf ihrer unternehmenseigenen Webseite eine Mitteilung, dass sie darauf aufmerksam gemacht worden sei, dass es bei einem ihrer Partner im Jahr 2019 zu einem Datenschutzverstoß gekommen sei. Die Hacker behaupteten, dass sie die Daten durch den Hack eines nicht näher benannten „Drittdienstleisters“ erbeutet hätten und der Datensatz aus dem Jahr 2019 stamme. Die Beklagte meldete den Cyberangriff am 10.11.2022 der zuständigen französischen Datenschutzbehörde (Commission Nationale de l’Informatique et des Libertés („CNIL“). Anfang 2023 erfolgte eine individuelle Betroffenenbenachrichtigung per E-Mail. In der Kommunikation riet die Beklagte den Nutzern insbesondere, ihre Passwörter als vorbeugende Sicherheitsmaßnahme zu ändern und die aktuellen Sicherheitsempfehlungen der Behörden zu beachten. 30

Ausweislich der Internetseite www.entfernt.com war die E-Mail-Adresse der Klägerin neben dem Datenschutzvorfall bei der Beklagten auch von vier weiteren Datenschutzvorfällen betroffen (Bl. 85, 540 GA). 31

Mit anwaltlicher E-Mail vom 29.06.2023 (Anlage K1, Bl. 36 ff. GA) forderte die Klägerin die Beklagte zur Auskunft, Unterlassung, Zahlung von Schadensersatz und Zahlung vorgerichtlicher Kosten auf. Mit E-Mail vom 21.07.2023 erteilte die Beklagte gegenüber der Klagepartei Auskunft gemäß Art. 15 DSGVO, Anlage B14, Bl. 308 ff. GA. Zuvor hatte die Beklagte um Fristverlängerung gebeten (Anlage K2) 32

Die Beklagte legte im Verfahren mit der Anlage B6 (Bl. 183 ff. GA) einen Auszug der Kundendatei der Klägerin vor. In der Klageerwiderung beantwortet sie vorgerichtlich gestellte Fragen (Bl. 170 ff. GA). 33

Die Klägerin behauptet im Wesentlichen, dass sie von dem Datenschutzvorfall betroffen sei und sie dadurch einen Kontrollverlust ihrer Daten mit weitreichenden Folgen im Alltagsleben erlitten habe. Deshalb stünden ihr Ansprüche gegen die Beklagte zu, insbesondere auf immateriellen Schadenersatz nach Art. 82 DSGVO. 34

Sie behauptet zudem was folgt: 35

„a.) Welche Art an Spam und Phishing erhält die Klägerseite 36

Die Klägerseite erhält Spam Nachrichten und Phishing-Angriffe per E-Mail. 37

b.) Anstieg des Spam und Phishing 38

Die Klägerseite erhält verstärkt Spam seit dem 10.12.2021. 39

Die Klägerseite erhält Phishing-Angriffe verstärkt seit dem 10.12.2020. 40

Es ergab auch einen erheblichen Anstieg des Spam /der Phishing-Angriffe: 41

Denn vor dem obengenannten Zeitraum erhielt die Klägerseite im Durchschnitt pro Woche 42

1-10 Spam-Mails 43

Nach dem Ansteigen der Spam- und Phishing-Angriffe (also nach dem obengenannten Zeitraum) ergeben sich im Durchschnitt pro Woche: 44

45

50+ Spam-Mails 40-50 Phishing-Mails.

Die Klägerseite hat erhebliche Sorge darüber, dass die abhanden gekommenen Daten für Spam genutzt werden. 46

Die Klägerseite hat erhebliche Sorge darüber, dass die abgefischten Daten zum Phishing 47

in Bezug auf die Social Media Accounts in Bezug auf das Bankkonto in Bezug auf den E-Mail-Account in Bezug auf den PayPal-Account 48

verwendet werden. 49

Die Klägerseite schätzt die Intensität der Sorge über den Datenkontrollverlust und die damit verbundenen Auswirkungen von einer Skala von 1 (wenig intensiv) bis 10 (stark intensiv) auf 9 im Durchschnitt ein. 50

Diese Sorge begleitet die Klägerseite so gut wie immer. 51

c.) Auswirkungen des Datenlecks 52

Das Datenleck hat folgende Auswirkungen auf die Klägerseite: 53

Nunmehr werden Spam-Emails durch Einstellungen im E-Mail-Account blockiert. Dies führt zu einem Zeitaufwand. 54

Emails deren Adressat der Klägerseite unbekannt sind, werden nicht gelesen, sondern gelöscht oder in den Spam Ordner verschoben. 55

Die Sorgen der Klägerseite über die Folgen des Datenlecks in Bezug auf Spam und insbesondere Phishing sind so groß, dass gelegentlich Schlafstörungen auftraten. 56

Passwörter hat die Klägerseite turnusmäßig geändert. 57

Aufgrund des Datenlecks prüft die Klägerseite nunmehr die Sicherheit der Accounts bzw. überprüft die Klägerseite regelmäßig wöchentlich, dass diese nicht gehackt wurden. Auch dies führt zu einem erheblichen Zeitaufwand. 58

Aufgrund des Datenlecks hat die Klägerseite die Mailadresse bereits geändert. Auch dies führte zu einem erheblichen Zeitaufwand, da z. B. andere über die neue Emailadresse informiert werden mussten. 59

Aufgrund des Datenlecks hat die Klägerseite die Privatsphäre-Einstellungen bei R. überprüft und geändert. 60

Aufgrund des Datenlecks und deren Auswirkungen ist die Klägerseite aufgrund von Angstzuständen in ärztlicher Behandlung. 61

Die Klägerseite ist auch immer noch aktuell von Spam- und Phishing Nachrichten betroffenen. Diese werden aktuell auf circa 40-50 pro Monat geschätzt.“ 62

Die Klägerin beantragte in der mündlichen Verhandlung am 08.10.2024, 63

1. Die Beklagte wird verurteilt, an die Klägerin als Ausgleich für Datenschutzverstöße und die Ermöglichung der unbefugten Ermittlung der Handynummer bzw. Mailadresse der Klägerseite 64

sowie weiterer personenbezogener Daten der Klägerseite wie Vorname, Nachname, Geschlecht, Geburtsdatum einen immateriellen Schadensersatz, dessen Höhe in das pflichtgemäße Ermessen des Gerichts gestellt wird, mindestens jedoch 3.000,00 € nebst Zinsen in Höhe von 5%-Punkten über dem Basiszinssatz seit Rechtshängigkeit zu bezahlen.

2. Es wird festgestellt, dass die Beklagte verpflichtet ist, der Klagepartei alle materiellen und immateriellen künftigen Schäden zu ersetzen, die der Klagepartei entstehen werden durch die unbefugte Veröffentlichung ihrer personenbezogenen Daten im Internet, die aufgrund eines Verschuldens der Beklagten und im Zeitraum zwischen 2019 und 2022 erfolgte. 65

3. Die Beklagte wird verurteilt, an die Klägerin für die Nichterteilung einer den gesetzlichen Anforderungen entsprechenden außergerichtlichen Datenauskunft im Sinne des Art. 15 DS-GVO einen weiteren immateriellen Schadensersatz, dessen Höhe in das Ermessen des Gerichts gestellt wird, den Betrag von 2.000,00 € aber nicht unterschreiten sollte, nebst Zinsen in Höhe von 5%-Punkten über dem Basiszinssatz seit Rechtshängigkeit zu bezahlen. 66

4. Die Beklagte wird verurteilt, der Klägerin Auskunft über die die Klägerin betreffenden weiteren personenbezogenen Daten zu erteilen, die durch Unbefugte erlangt werden konnten, namentlich welche Daten außer der Telefonnummer der Klägerseite durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten unbefugt erlangt werden konnten. 67

5. Die Beklagte wird 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 sechs Monaten, im Wiederholungsfall bis zu 2 Jahren, zu unterlassen zu unterlassen, personenbezogene Daten der Klägerseite, namentlich Telefonnummer und Mailadresse sowie das Nutzerprofil Dritten über eine API-Schnittstelle zugänglich zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzunehmen. 68

6. Die Beklagte wird weiter verurteilt, an die Klägerin vorgerichtliche Rechtsanwaltskosten in Höhe von 1.295,43 € zzgl. Zinsen in Höhe von 5%-Punkten über dem Basiszinssatz per anno seit Rechtshängigkeit zu bezahlen. 69

Im nicht nachgelassenen Schriftsatz vom 30.12.2024 formulierte die Klägerin davon abweichende Anträge zu 2), zu 4) und zu 5). 70

Die Beklagte beantragt, 71

die Klage abzuweisen. 72

Die Beklagte verteidigt sich im Wesentlichen damit, alle technisch-organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten ihrer Nutzer eingehalten zu haben. Daten seien bei einem ehemaliger Dienstleister im Rahmen eines Cyberangriffs abhanden gekommen, nachdem drei der Mitarbeiter die von dem Vorfall betroffenen Datensätze von einer Produktivumgebung („production environment") in eine vom Dienstleister außerhalb der Vertragsbeziehung mit der Beklagten betriebene Nicht-Produktivumgebung („non-production environment“) überführt hätten. 73

Die Beklagte bestreitet, dass die Klägerin und ihre Daten von dem streitgegenständlichen Hackerangriff überhaupt betroffen gewesen seien. Sie behauptet, P. Inc. habe der Beklagten am 22. Februar 2023 bestätigt, dass sämtliche Daten der Beklagten sofort nach 74

Vertragsbeendigung gelöscht worden seien. Sie behauptet zudem, P. Inc. habe sodann im Juni 2023 eingeräumt, dass drei ihrer Mitarbeiter die von dem Vorfall betroffenen Datensätze von einer Produktivumgebung („production environment“) in eine vom Dienstleister außerhalb der Vertragsbeziehung mit der Beklagten betriebene Nicht-Produktivumgebung („non-production environment“) überführt hatten. Dieser Vorgang sei vertraglich nicht gestattet gewesen und die Beklagte habe von diesem Vorgang keine Kenntnis gehabt.

Die Beklagte behauptet, der streitgegenständliche Vorfall habe kurz vor der Veröffentlichung der Daten, jedenfalls aber erst nach Beendigung der Zusammenarbeit mit dem oben genannten Dienstleister stattgefunden. 75

Es liege kein Datenschutzverstoß vor. Der Klägerin sei kein Schaden entstanden. Auch die übrigen geltend gemachten Ansprüche bestünden nicht. 76

Die Klageschrift ist den Prozessbevollmächtigten der Beklagten am 30.01.2024 zugestellt worden. 77

Entscheidungsgründe: 78

Die Klage ist teilweise unzulässig und im Übrigen nur teilweise begründet. 79

I. Der Klageantrag zu 5) in der maßgeblichen Antragsfassung ist unzulässig. Im Übrigen ist die Klage zulässig. 80

1. Das Landgericht Köln ist international, örtlich und sachlich zuständig, was aus der Anwendung der Artt. 7 Nr. 1, 18 Abs. 1 EuGVVO, Artt. 79 Abs. 2 S. 2, 82 Abs. 6 DSGVO, § 44 Abs. 1 S. 2 BDSG und §§ 23 Nr. 1, 71 Abs. 1 GVG folgt. 81

2. Dem Unterlassungsantrag zu 5) fehlt es hingegen an der hinreichenden Bestimmtheit gem. § 253 Abs. 2 Nr. 2 ZPO. 82

a) Dabei war zunächst die Antragsänderung im nicht nachgelassenen Schriftsatz vom 30.12.2024 unbeachtlich. Denn diese erfolgte nach Schluss der mündlichen Verhandlung. Zwar handelt es sich bei dem Antrag nicht um ein Angriffsmittel, das nach § 296a ZPO präkludieren könnte, sondern um den Antrag selbst. Die Anträge werden aber in der mündlichen Verhandlung gestellt und können danach nicht mehr einseitig geändert werden. Ein Grund zur Wiedereröffnung der mündlichen Verhandlung nach § 156 ZPO ist nicht ersichtlich. Dieser liegt insbesondere nicht darin begründet, dass der BGH im Grundsatzurteil vom 18. November 2024 - VI ZR 10/24 - zum Scraping bei Meta zu diesem Thema den Klägervertretern eindeutige „Segelanweisungen“ gegeben hat. Die Zweifel an der Zulässigkeit der Anträge waren bereits zuvor von der Beklagten hinreichenden deutlich schriftsätzlich vorgetragen worden, sodass bereits in der mündlichen Verhandlung ein zulässiger Antrag hätte gestellt werden können. Die entsprechenden Rechtsgrundsätze zur Bezugnahme auf eine konkrete Verletzungsform sind seit langem höchstrichterlich geklärt (vgl. etwa BGH, Urteil vom 7. 4. 2011 - I ZR 34/09, GRUR 2011, 742 - Leistungspakete im Preisvergleich). 83

b) Die Klage ist demnach insoweit unzulässig, soweit der Kläger die Beklagte auf Unterlassung der Zugänglichmachung seiner personenbezogenen Daten, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzunehmen, in Anspruch nimmt. 84

Ein Klageantrag ist hinreichend bestimmt (§ 253 Abs. 2 Nr. 2 ZPO), wenn er den erhobenen Anspruch konkret bezeichnet, dadurch den Rahmen der gerichtlichen Entscheidungsbefugnis (§ 308 ZPO) absteckt, Inhalt und Umfang der materiellen Rechtskraft der begehrten 85

Entscheidung (§ 322 ZPO) erkennen lässt, das Risiko eines Unterliegens des Klägers nicht durch vermeidbare Ungenauigkeit auf den Beklagten abwälzt und eine Zwangsvollstreckung aus dem Urteil ohne eine Fortsetzung des Streits im Vollstreckungsverfahren erwarten lässt (BGH, Urteil vom 9. März 2021 - VI ZR 73/20, VersR 2021 , 795 Rn. 15). Dies bedeutet bei einem Unterlassungsantrag insbesondere, dass dieser nicht derart undeutlich gefasst sein darf, dass die Entscheidung darüber, was dem Beklagten verboten ist, letztlich dem Vollstreckungsgericht überlassen bleibt (vgl. BGH, Urteile vom 28. Juli 2022 -1 ZR 205/20, VersR 2022, 1389 Rn. 12; vom 2. Juni 2022 - I ZR 140/15, BGHZ 234, 56 Rn. 26).

Die Verwendung auslegungsbedürftiger Begriffe im Klageantrag ist zulässig, wenn über ihren Sinngehalt zwischen den Parteien kein Streit besteht und objektive Maßstäbe zur Abgrenzung vorliegen, oder wenn der Kläger den auslegungsbedürftigen Begriff hinreichend konkret umschreibt und gegebenenfalls mit Beispielen unterlegt oder sein Begehren an der konkreten Verletzungshandlung ausrichtet (BGH, Urteile vom 2. Juni 2022 - I ZR 140/15, BGHZ 234, 56 Rn. 26; vom 9. September 2021 - I ZR 113/20, GRUR 2021, 1425 Rn. 12 mwN). 86

Demgegenüber sind Unterlassungsanträge, die lediglich den Wortlaut eines Gesetzes wiederholen, grundsätzlich als zu unbestimmt und damit unzulässig anzusehen. Abweichendes kann gelten, wenn entweder bereits der gesetzliche Verbotstatbestand selbst entsprechend eindeutig und konkret gefasst oder der Anwendungsbereich einer Rechtsnorm durch eine gefestigte Auslegung geklärt ist, oder wenn der Kläger hinreichend deutlich macht, dass er nicht ein Verbot im Umfang des Gesetzeswortlauts beansprucht, sondern sich mit seinem Unterlassungsbegehren an der konkreten Verletzungshandlung orientiert. Die Bejahung der Bestimmtheit setzt in solchen Fällen allerdings grundsätzlich voraus, dass zwischen den Parteien kein Streit darüber besteht, dass das beanstandete Verhalten das fragliche Tatbestandsmerkmal erfüllt. Die Wiedergabe des gesetzlichen Verbotstatbestands in der Antragsformulierung ist auch unschädlich, wenn sich das mit dem selbst nicht hinreichend klaren Antrag Begehrte im Tatsächlichen durch Auslegung unter Heranziehung des Sachvortrags des Klägers eindeutig ergibt und die betreffende tatsächliche Gestaltung zwischen den Parteien nicht infrage gestellt ist, sondern sich ihr Streit ausschließlich auf die rechtliche Qualifizierung der angegriffenen Verhaltensweise beschränkt. Eine auslegungsbedürftige Antragsformulierung kann im Übrigen hinzunehmen sein, wenn dies zur Gewährleistung effektiven Rechtsschutzes erforderlich ist (st. Rspr.; vgl. nur BGH, Urteile vom 28. Juli 2022 - I ZR 205/20, VersR 2022, 1389 Rn. 12; vom 22. Juli 2021 - I ZR 194/20, GRUR 2021 , 1534 Rn. 34 mwN; *alles Vorstehende zitiert nach BGH, Urteil vom 18. November 2024 - VI ZR 10/24, Rn. 52 ff., zum Scraping bei Meta*). 87

Nach diesen Grundsätzen ist der Klageantrag zu 5) nicht hinreichend bestimmt. Er lässt sich auch unter Heranziehung des Klagevorbringens nicht in einer Weise auslegen, dass der Kläger ein hinreichend bestimmtes Unterlassen begehrt. 88

Insbesondere nimmt der Unterlassungsantrag keine konkrete Verletzungsform in Bezug. Die an Art. 32 Abs. 1 DSGVO und damit an den bloßen Gesetzeswortlaut angelehnte Formulierung der „nach dem Stand der Technik möglichen Sicherheitsmaßnahmen“ ist für sich betrachtet zu unbestimmt. Der Antrag lässt nicht erkennen, durch welche konkrete Maßnahme die Beklagte gegen die Datenschutz-Grundverordnung verstoßen hat. Spiegelbildlich bleibt auch vollkommen unklar, welche Sicherheitsmaßnahmen insoweit zur Verhinderung eines etwaigen Datenschutzverstoßes geboten wären. Im Ergebnis würde ein erheblicher Teil des Streits in ein gedachtes Zwangsvollstreckungsverfahren nach § 890 ZPO verlagert, was nicht zulässig ist. 89

3. Im Übrigen bestehen keine Zulässigkeitsbedenken. Auch ist das Feststellungsinteresse für den Klageantrag zu 2) gegeben (vgl. dazu BGH, Urteil vom 18. November 2024 - VI ZR 10/24, Rn. 46 ff., zum Scraping bei Meta). 90

II. Die Klage ist nur teilweise begründet. 91

Die Klageanträge zu 1) und 6) haben in geringem Umfang und der Klageantrag zu 2) insgesamt Erfolg. Im Übrigen ist die Klage unbegründet. 92

1. Klageantrag zu 1) – immaterieller Schadensersatz 93

Der Klägerin hat gegen die Beklagte einen Anspruch auf Zahlung von immateriellen Schadensersatz gemäß Art. 82 Abs. 1 DSGVO wegen Datenschutzverstößen im Zusammenhang mit dem unstreitigen Datenschutzvorfall bei der Unterauftragnehmerin der Klägerseite. Dieser beläuft sich in der Höhe jedoch nur auf 100,- €. 94

a) Die Beklagte ist als Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO passivlegitimiert. Der Verantwortliche (und Auftragsverarbeiter) haftet im Grundsatz nach Art. 82 DSGVO für das Handeln seiner Auftragsverarbeiter und deren Mitarbeiter jedenfalls dann, wenn dem Mitarbeiter erst durch die ihm vom Verantwortlichen oder Auftragsverarbeiter übertragene Tätigkeit die Gelegenheit gegeben wurde, auf die Rechtsgüter der betroffenen Person einzuwirken. Der Verantwortliche haftet auch, wenn der Auftragsverarbeiter die Weisungen des Verantwortlichen ausführt und dadurch ein Schaden entsteht. Missachtet der Auftragsverarbeiter eine rechtmäßige Weisung des Verantwortlichen, haftet der Verantwortliche auch hierfür. Zwar besteht in diesem Fall auch eine Haftung des Auftragsdatenverarbeiters. Der Verantwortliche kann den Betroffenen aber nicht auf dessen vorrangige Inanspruchnahme verweisen, weil dies einem „wirksamen Schadensersatz“ im Sinne des Art. 82 Abs. 4 DSGVO (vgl. auch Erwägungsgrund 146 S. 6) entgegenstünde. Ein Abschieben der Haftung auf den Auftragsverarbeiter widerspricht auch dem Grundgedanken der Auftragsverarbeitung, wonach der Verantwortliche zwar ohne Weiteres Dritte einschalten darf, aber gegenüber der betroffenen Person verantwortlich bleibt. Der Auftragsverarbeiter ist letztlich – mit einigen formalen und inhaltlichen Anforderungen, die aus der fehlenden arbeitsrechtlichen Weisungsbefugnis und tatsächlichen Kontrollmöglichkeit herrühren – wie ein sonstiger Mitarbeiter zu behandeln (OLG Dresden, Urteil vom 15.10.2024 – 4 U 940/24, GRUR-RS 2024, 28974, Rn. 22 mwN). 95

b) Die Klägerin ist aktivlegitimiert. Sie war ausweislich der von der Beklagten in der Klageerwiderung vorgelegten Daten zum streitgegenständlichen Zeitpunkt, jedenfalls Anfang 2019, Kundin der Beklagten. Entsprechend wurden personenbezogene Daten der Klägerseite bei der Beklagten verarbeitet. 96

Das Gericht legt es seiner Entscheidung dabei zu Grunde, dass diese Daten an die P. Inc. weitergegeben worden sind und dort im Rahmen der Auftragsdatenverarbeitung verarbeitet worden sind. Es geht auch davon aus, dass die Daten sodann bei der P. Inc. von Unbekannten abgegriffen und im Darknet veröffentlicht worden sind. Die Klägerin ist demnach von dem Datenschutzverstoß betroffen. 97

Dabei hat das Gericht beachtet, dass die Beklagte ausweislich ihrer Verteidigung „in Bezug auf die Klagepartei (…) keine positive Kenntnis darüber [habe], ob und falls ja, welche ihrer Informationen tatsächlich Gegenstand eines unberechtigten Zugriffs wurden.“ (vgl. Klageerwiderung S.6, Bl. 75 GA). Jedoch stellt die Beklagte selbst den Sachverhalt so dar, dass der betroffene Datensatz aus dem Jahr 2019 stammen soll. Dies führt jedoch zu der 98

Schlussfolgerung, dass die Daten der Klägerin, die bereits seit Mitte 2018 bei der Beklagten registriert war, zu diesem betroffenen Datensatz gehören. Vor diesem Hintergrund hält das Gericht die Betroffenheit im Ausgangspunkt für unstreitig. Es hätte der Beklagte oblegen, darzulegen ob und wieso gerade die Daten der Klägerin nicht zum betroffenen Datensatz gehören sollen. Dies müsste ihr nach eigener Schilderung der Aufklärungsarbeit nach Bekanntwerden des Datenleaks bzw. der Veröffentlichung um Darknet auch ohne weiteres möglich sein. Insbesondere müsste sie hierfür keine illegalen Tätigkeiten zur Beschaffung der Leakliste vornehmen. Denn wenn die Beklagte das Datenleck bei der P. Inc. verorten kann, so müsste ihr aus eigenem Wissen auch bekannt worden, welche Daten dorthin übertragen und dort verarbeitet worden sind – und welche Daten nicht betroffen sind. Dies gilt umso mehr, als dass die Beklagte selbst ausschließt, dass es zu anderweitigen Sicherheitslücken in ihren Systemen gekommen ist.

c) Der Beklagten ist mindestens ein Datenschutzverstoß vorzuwerfen. 99

aa) Die Beklagte hat gegen die ihr obliegende Pflicht zur sorgfältigen Überwachung des von ihr beauftragten externen Auftragsdatenverarbeiters verstoßen, Art. 28, 32 DSGVO (OLG Dresden, Urteil vom 15.10.2024 – 4 U 940/24, aaO, Rn. 23 ff., was nachfolgend dargestellt wird). 100

Art. 28 Abs. 1 DSGVO regelt unmittelbar nur die Anforderungen an die Auswahl des Auftragsverarbeiters durch den Verantwortlichen. Dieser darf nur solche Auftragnehmer als Auftragsverarbeiter beauftragen, „die hinreichende Garantie dafür bieten, dass geeignete technische und organisatorische Maßnahmen“ im Einklang mit der DSGVO durchgeführt werden. Dies führt aber nicht nur zu einer Pflicht zur sorgfältigen Auswahl, sondern auch zu einer Pflicht zur sorgfältigen Überwachung des Auftragsverarbeiters durch den Verantwortlichen. Diese Pflicht zur Überwachung des Auftragsverarbeiters – im Anschluss an dessen Auswahl – ist in Art. 28 Abs. 1 DSGVO zwar nicht ausdrücklich geregelt, ergibt sich jedoch aus der Formulierung der Norm („arbeitet […] nur mit“). Absatz 3 lit h) setzt eine solche Kontrollpflicht voraus, was auch die ordnungsgemäße Datenlöschung betrifft. Zugleich enthält er eine Verpflichtung der Vertragsparteien, die Details zu den Prüfrechten auszugestalten und hierdurch eine effektive Kontrolle durch den Verantwortlichen sicherzustellen (Schaffland/Wiltfang, Datenschutz-Grundverordnung (DS-GVO)/Bundesdatenschutzgesetz (BDSG), 8. Ergänzungslieferung 2024, Art. 28 EUV 2016/679, Rn. 61). De facto ist die Pflicht zur Überwachung daher auch ohne konkrete zeitliche Vorgaben als Dauerpflicht zu verstehen (vgl. Plath in: Plath, DSGVO/BDSG/TTDSG, 4. Auflage 2023, Rz. 17 mwN). Durch diese vertragliche Ausgestaltung werden aber nicht nur die Pflichten des Auftragsdatenverarbeiters, sondern auch die korrespondierenden Prüfpflichten des Unternehmers konkretisiert. Der Auftragsverarbeiter ist nach Vertragsende – als Ausfluss der allgemeinen Grundsätze der „Rechtmäßigkeit“, (Art. 5 Abs. 1 lit. (a) DSGVO), der „Datenminimierung“ (Art. 5 Abs. 1 lit. (c) DSGVO) sowie der Speicherbegrenzung (Art. 5 Abs. 1 (e) DSGVO) – verpflichtet, alle noch vorhandenen personenbezogenen Daten entweder zu löschen oder zurückzugeben (vgl. Paal/Pauly/Martini, 3. Aufl. 2021, DS-GVO Art. 28 Rn. 22, 23, beck-online mit Verweisen auf Spoerr in BeckOK DatenschutzR DS-GVO Art. 28 Rn. 78). Dies entspricht Art. 9 der Vereinbarung in Anlage B2a. 101

Die Anforderungen an Auswahl und Überwachung dürfen dabei in der Praxis zwar nicht überspannt werden. Wählt ein Unternehmen z.B. einen führenden und am Markt als zuverlässig bekannten IT-Dienstleister aus, so darf es grundsätzlich auf dessen Fachwissen und Zuverlässigkeit vertrauen, ohne dass etwa eine – vollkommen praxisfremde – Vor-Ort- 102

Kontrolle erforderlich wäre (Schaffland/Wiltfang aaO.). Gesteigerte Anforderungen ergeben sich indes, soweit z.B. große Datenmengen oder besonders sensible Daten gehostet werden sollen (Plath, a.a.O., Rz. 18). Diese gesteigerten Kontrollpflichten gelten auch außerhalb der Verarbeitung personenbezogener Daten nach Art. 9, 10 DSGVO. Ungeachtet der Frage, ob die von dem zwischen der Beklagten und dem Autragsdatenverarbeiter geschlossenen Vertrag erfassten Daten auch Daten über das Nutzerverhalten und hieraus zu erstellende Profile beinhalteten, betraf die Verarbeitung vorliegend jedenfalls nicht unbedeutende Datenmengen, deren Verlust potentiell vielen Millionen Nutzern Schaden zufügen konnte. Infolgedessen war die Beklagte auch nach Vertragsbeendigung zu einer Überwachung ihres Auftragsdatenverarbeiters dahingehend angehalten, dass dieser die ihm zur Verfügung gestellten Daten tatsächlich löscht und hierüber eine aussagekräftige Bescheinigung ausstellt. Diese durch die DSGVO gesetzlich aufgestellten Anforderungen werden in Ziff. 9 der am 18.7.2019 geschlossenen Zusatzvereinbarung (Anlage B 2a) präzisiert (siehe wörtliches Zitat im Tatbestand).

In Ergänzung hierzu regelt Ziff. 10.1 der Anlage B2a das Recht der Beklagten, von dem Auftragsdatenverarbeiter „alle erforderlichen Informationen“ verlangen zu dürfen, „soweit dies vernünftigerweise erforderlich ist“. Folgerichtig war die Beklagte zum einen verpflichtet, von ihrem Wahlrecht nach Ziff. 9.1. Gebrauch zu machen, d.h. entweder die Rückübertragung oder die Löschung der von dem Auftragsdatenverarbeiter gehosteten Daten innerhalb der dort genannten Fristen zu verlangen. Zum anderen war sie gehalten, die Erfüllung der den Auftragsdatenverarbeiter hiernach treffenden Verpflichtungen zu kontrollieren, also die nach dem Vertrag erforderlichen Bestätigungen einzuholen, bei deren Ausbleiben innerhalb der 21-Tage Frist die Vorlage unverzüglich anzumahnen und ggf. auch eine Vorort-Prüfung nach Art. 10 des Nachtrags vorzunehmen. Nichts davon ist hier geschehen. Dem Vortrag der Beklagten lässt sich bereits nicht entnehmen, dass diese gegenüber dem Auftragsdatenverarbeiter ihr Wahlrecht gem. Ziff. 9.1. des Nachtrags überhaupt ausgeübt hätte. 103

Insbesondere hat sie aber dadurch gegen ihre Kontrollpflichten aus Art. 28 DSGVO verstoßen, dass sie nicht nach Ablauf der vertraglich geregelten 21-tägigen Frist von ihrer Auftragsverarbeiterin die ausdrückliche schriftliche Bestätigung einer tatsächlich durchgeführten Löschung aller bei dieser vorhandenen Datensätze angefordert hat, die eine detaillierte Auflistung der gelöschten Daten enthielt. Die E-Mail des Auftragsdatenverarbeiters vom 9.12.2020 (Anlage B4) enthielt lediglich die Ankündigung einer bevorstehenden, nicht aber die Bestätigung einer erfolgten Löschung. Die bloße Ankündigung einer Maßnahme ist jedoch nicht gleichwertig zu einer Bestätigung über deren Ausführung. Es ist allgemein bekannt, dass gleich ob in kleinen oder großen Unternehmen anstehende Vorgänge aufgeschoben und in der Folge auch vergessen werden können. Indem die Bestätigung der tatsächlichen Durchführung einer vertraglich festgelegten Aufgabe eingefordert wird, minimiert der Verantwortliche das Risiko, dass es beim Auftragsverarbeiter bei der bloßen Ankündigung eines Tätigwerdens bleibt und sorgt zugleich dafür, dass der Auftragsverarbeiter in seiner eigenen Sphäre überprüft, ob die vertraglich übernommene Verpflichtung tatsächlich gewissenhaft erfüllt wurde – auch um das eigene Haftungsrisiko zu minimieren. 104

Die als Anlage B4 vorgelegte Löschungsankündigung des Auftragsdatenverarbeiters erfüllte aber auch unabhängig hiervon nicht die zum Zwecke und zur Sicherstellung der gesetzlichen Pflichten vertraglich festgelegten Anforderungen, weil sie sich lediglich auf „your site and all the data on the site“, d.h. die unmittelbar von der Beklagten zur Verfügung gestellte Website einschließlich der dort befindlichen Daten, nicht jedoch auf die „Löschung aller anderen 105

Kopien der personenbezogenen Daten des Unternehmens, die vom Anbieter … verarbeitet wurden“ erstreckte, wie es Ziff. 9.1. vorsieht.

Angesichts dessen hätte sich die Beklagte mit dieser weder formal noch inhaltlich hinreichenden Ankündigung nicht zufrieden geben dürfen, sondern auf eine vollständige und rechtzeitige Löschungsbestätigung hinwirken müssen. Wäre diese auf Anforderung nicht unverzüglich vorgelegt worden, hätte sie ggf. eine nach Ziff. 10.1. des Nachtrags vorgesehene Vor-Ort Kontrolle durchführen müssen. Dies ist indes unstreitig nicht geschehen. Eine Nachfrage beim Auftragsdatenverarbeiter ist nach dem eigenen Vorbringen der Beklagten nicht vor dem Jahr 2023 erfolgt. Die als Anlage B5 vorgelegte, als „Declaration of Data Destruction“ bezeichnete E-Mail vom 22.3.2023 liegt aber weit außerhalb eines für diese nach Art. 28 DSGVO erforderliche Kontrolle vertretbaren Prüfzeitraums. Ob sie eine hinreichende Bescheinigung im Sinne von Ziff. 9 Abs. 1 des Nachtrags enthält, kann schon aus diesem Grund dahinstehen. 106

Schließlich kann auch die Kausalität dieser Kontrollpflichtenverletzung für den streitgegenständlichen Hacking-Vorfall nicht verneint werden. Ausgehend vom Regelfall des redlichen Auftragsdatenverarbeiters muss vielmehr angenommen werden, dass die Mitarbeiter der Firma P. Inc. spätestens auf eine Nachfrage der Beklagten reagiert und die bei ihnen noch vorhandenen Daten gelöscht hätten; jedenfalls die Ankündigung einer Vorort-Kontrolle hätte dazu geführt, dass entsprechende Aktivitäten in die Wege geleitet worden wären. Zu einem Abgreifen der Daten, das nach dem Vorbringen der Beklagten erst im Jahr 2022 erfolgt ist, wäre es dann nicht gekommen. Dass der Dienstleister unter dem Eindruck des erfolgten und ihm bekannten Datenlecks und angesichts der zu erwartenden Haftungsansprüche am 22.3.2023 nachträglich eine unrichtige Löschungsbescheinigung erteilt hat, lässt keinen Rückschluss darauf zu, dass er dies auch im Jahr 2020 getan hätte. Anders wäre dies lediglich dann, wenn der Auftragsdatenverarbeiter selbst unredlich gehandelt und die Daten deshalb nicht gelöscht hätte, um sie selbst später weiter zu veräußern oder für eigenen Zwecke zu verarbeiten. Anhaltspunkte für einen solchen Verdacht sind von der hierfür beweisbelasteten Beklagten indes nicht aufgezeigt worden. Nur in einem solchen Fall käme auch ein Auftragverarbeiterexzess gem. Art. 82 Abs. 3 DSGVO in Betracht, der die Verantwortlichkeit der Beklagten entfallen ließe. Das bloß versehentliche Nichtlöschen der Daten, das noch dazu durch eine unzureichende Kontrolle seitens der Beklagten maßgeblich erleichtert wurde, hält sich jedoch noch im Rahmen des Erwartbaren und erfüllt damit die Voraussetzungen des Art. 82 Abs. 3 DSGVO nicht. 107

bb) Ergänzend neigt das Gericht dazu, muss es aber angesichts des oben dargestellten Verstoßes nicht entscheiden, dass die Beklagte bereits einen Verstoß gegen Art. 28 DSGVO begangen hat, indem die Daten überhaupt an die P. Inc. übertragen worden sind, obwohl keine entsprechende hinreichende Auftragsdatenvereinbarung vorgetragen ist. 108

Dabei ergeben sich die Anforderungen an die Übertragung von Daten auf Auftragsverarbeiter aus Art. 28 DSGVO. Hiernach setzt die Verarbeitung von Daten durch Auftragsverarbeiter (und entsprechend die Übergabe der Daten an den Auftragsverarbeiter) voraus, dass zwischen der Beklagten und dem Auftragsverarbeiter ein Vertrag oder ein anderes Rechtsinstrument gem. Art. 28 Abs. 3 DSGVO vorliegt, der die dort im Einzelnen aufgezählten Maßnahmen und Gewährleistungen vorsieht. Entsprechendes gilt für eventuelle Unterauftragsverarbeiter: diesen muss ebenfalls verbindlich durch Vertrag oder ein anderes Rechtsinstrument dieselben Datenschutzpflichten auferlegt worden sein wie dem Auftragsverarbeiter selbst, § 28 Abs. 4 DSGVO. Fehlt es an diesen Voraussetzungen, so stellt sich auch die Übermittlung der Daten von dem Verantwortlichen an den 109

Auftragsverarbeiter oder Unterauftragsverarbeiter als rechtswidrig dar (vgl. hierzu etwa BeckOK DatenschutzR/Spoerr, 49. Ed. 1.8.2024, DS-GVO Art. 28 Rn. 29-32.1 m.w.N. zur dogmatischen Herleitung; Kühling/Buchner/Hartung, 4. Aufl. 2024, DS-GVO Art. 28 Rn. 61-63: „Umgekehrt ist eine fehlende oder unvollständige Vereinbarung ein eigener Normverstoß (…)“ / zitiert aus LG Lübeck, Urteil vom 04.10.2024 – 15 O 216/23, GRUR-RS 2024, 26215, Rn. 64).

Diesen Anforderungen wird die vorgetragene Vertragslage nicht gerecht. Die oben bereits angesprochene Anlage B2a ist zwischen der Beklagten und der V. O. Inc. geschlossen, nicht aber zwischen der Beklagten und der P. Inc. Die in Anlage B2a für weitere Unterauftragsverarbeiter geltenden Regelungen in Ziffer 5 (oben im Tatbestand zitiert) wurden offenbar nicht vertragsgemäß umgesetzt, andernfalls wäre es der Beklagte ohne weiteres möglich gewesen die nach Ziff. 5.3 lit. b) & d) notwendigen Vertragskopien vorzulegen (vgl. zu diesem Aspekt ausführlich LG Lübeck aaO). 110

cc) Ob daneben die Beklagte ihrer Pflicht zur Einhaltung aller erforderlichen technischen und organisatorischen sowie personellen Sicherheitsstandards im eigenen Hause nachgekommen ist, kann offenbleiben. Gleiches gilt im Ergebnis für die Einhaltung der technischen Sicherheitsstandards im Hause des (Unter-) Auftragsdatenverarbeiters P. Inc. Offenbleiben kann ebenfalls, ob die Beklagte ihre Benachrichtigungspflicht aus Art. 34 DSGVO gegenüber der Klagepartei, aus Art. 33 DSGVO gegenüber der Aufsichtsbehörde oder die Auskunftspflicht nach Art. 15 DSGVO verletzt hat, denn ein kausaler Schaden der Klagepartei, der auf der Verletzung von Benachrichtigungspflichten beruhen könnte, ist nicht ersichtlich (vgl. OLG Dresden, Urteil vom 15.10.2024 – 4 U 940/24, aaO, Rn. 30, 32). 111

d) Die nach Art. 82 Abs. 3 DSGVO notwendige Kausalität des Datenschutzverstoßes für das sodann schadensbegründende Ereignis in Form des Hackerangriffs und der Veröffentlichung von Daten im Darknet ist gegeben (siehe auch bereits oben unter lit. c), aa)). Jedenfalls kann die Beklagte den in Art. 82 Abs. 3 DSGVO ihr obliegenden Nachweis der in jedweder Hinsicht fehlenden Verantwortlichkeit nicht führen. Durch die Einhaltung der gebotenen Kontrolle der Löschung bei der P. Inc. wäre das Datenleck in seiner streitgegenständlichen Ausprägung wohl vermieden worden. Da insoweit die Kausalität positiv bejaht werden kann, kommt es auf die Verteidigung zu einer fehlenden Kausalität nicht an. 112

e) Die Beklagte hat den oben dargelegten Datenschutzverstoß in Form der unzureichenden Kontrolle der Löschung der Daten bei der P. Inc. auch zu vertreten. Dieser Verstoß erfolgte jedenfalls fahrlässig, weil die gebotenen Sorgfaltsanforderungen mindestens die Einhaltung der oben dargelegten vertraglich vorgesehenen Kontrolle nach 21 Tagen umfassen. Diese hat die Beklage offenbar außer Acht gelassen und sich stattdessen mit einer bloßen Ankündigung der Datenlöschung (Anlage B4) zufrieden gegeben. Angesichts des festgestellten Vertretenmüssens bedarf es keiner Entscheidung des juristischen Meinungsstreits, ob Art. 82 DSGVO überhaupt ein Verschuldenserfordernis hat (vgl. die Darstellung des Meinungsstands bei LG Lübeck, Urteil vom 04.10.2024 – 15 O 216/23, GRUR-RS 2024, 26215, Rn. 71). 113

f) Es liegt auch ein ersatzfähiger Schaden im Sinne von Art. 82 Abs. 1 DSGVO vor. 114

Grundsätzlich ermöglicht Art. 82 Abs. 1 DSGVO den Ersatz materieller und immaterieller Schäden. Ein materieller Vermögensschaden wurde von der Klägerin nicht vorgetragen. Sie beruft sich jedoch erfolgreich auf das Vorliegen eines immateriellen Schadens. 115

116

Diesen Schadensersatz schätzt das Gericht jedoch lediglich in Höhe von 100,- € wegen des bei der Klägerin eingetretenen Kontrollverlusts. Für einen mit der Klage geltend gemachten Anspruch in Höhe von 3000,- € fehlt es hingegen an einem weitergehenden immateriellen Schaden.

aa) Art. 82 Abs. 2 DSGVO, der die Haftungsregelung, deren Grundsatz in Abs. 1 dieses Artikels festgelegt ist, präzisiert, übernimmt die drei Voraussetzungen für die Entstehung des Schadenersatzanspruchs, nämlich eine Verarbeitung personenbezogener Daten unter Verstoß gegen die Bestimmungen der DSGVO, ein der betroffenen Person entstandener Schaden und ein Kausalzusammenhang zwischen der rechtswidrigen Verarbeitung und diesem Schaden (so EuGH Urteil vom 04.05.2023 – C – 300/21, Rn 36 – juris). Der europäische Gerichtshof stützt sich auf den 146. Erwägungsgrund, der auf „Schäden“ abstellt, „die einer Person aufgrund einer Verarbeitung entstehen“. Zwar muss der Schaden nicht eine gewisse Erheblichkeit erreichen, jedoch besteht ein Nachweiserfordernis für immaterielle Schäden durch die betroffene Person (vgl. EuGH, Urteil vom 04.05.2023 – C – 300/21, 49, 50 – juris). Allerdings muss der Schaden tatsächlich und sicher entstanden sein (vgl. EuGH, Urteil vom 04.04.2017 – C – 337/15, Rn 91 – juris). Hierbei hat der Europäische Gerichtshof in einem behaupteten Verlust des Vertrauens in eine Institution keinen ersatzfähigen immateriellen Schaden gesehen (vgl. EuGH, Urteil vom 04.04.2017 – C – 337/15, Rn 95 – juris / zitiert nach OLG Dresden, Endurteil vom 10.12.2024 – 4 U 808/24, GRUR-RS 2024, 35688, Rn. 15). 117

Der Kontrollverlust der Daten der Klägerin hat zu einem immateriellen Schaden im Sinne von Art. 82 DSGVO bei der Klagepartei geführt. 118

Der Bundesgerichtshof hat im Urteil vom 18.11.2024 (VI ZR 10/24) insofern folgendes ausgeführt: 119

„Der Begriff des „immateriellen Schadens“ ist in Ermangelung eines Verweises in Art. 82 Abs. 1 DSGVO auf das innerstaatliche Recht der Mitgliedstaaten im Sinne dieser Bestimmung autonom unionsrechtlich zu definieren (st. Rspr., EuGH, Urteile vom 20. Juni 2024 – C-590/22, DB 2024, 1676 Rn. 31 – PS GbR; vom 25. Januar 2024 – C-687/21, CR 2024,160 Rn. 64 – MediaMarkt-Saturn; vom 4. Mai 2023 – C-300/21, VersR 2023, 920 Rn. 30 und 44 – Österreichische Post). Dabei soll nach ErwG 146 Satz 3 DSGVO der Begriff des Schadens weit ausgelegt werden, in einer Art und Weise, die den Zielen dieser Verordnung in vollem Umfang entspricht. Der bloße Verstoß gegen die Bestimmungen der Datenschutz-Grundverordnung reicht nach der Rechtsprechung des Gerichtshofs jedoch nicht aus, um einen Schadensersatzanspruch zu begründen, vielmehr ist darüber hinaus – im Sinne einer eigenständigen Anspruchsvoraussetzung – der Eintritt eines Schadens (durch diesen Verstoß) erforderlich (st. Rspr., vgl. EuGH, Urteile vom 20. Juni 2024 – C-590/22, DB 2024, 1676 Rn. 25 – PS GbR; vom 11. April 2024 – C-741/21, NJW 2024, 1561 Rn. 34 – juris; vom 4. Mai 2023 – C-300/21, VersR 2023, 920 Rn. 42 – Österreichische Post). Weiter hat der Gerichtshof ausgeführt, dass Art. 82 Abs. 1 DSGVO einer nationalen Regelung oder Praxis entgegensteht, die den Ersatz eines immateriellen Schadens im Sinne dieser Bestimmung davon abhängig macht, dass der der betroffenen Person entstandene Schaden einen bestimmten Grad an Schwere oder Erheblichkeit erreicht hat (EuGH, Urteile vom 20. Juni 2024 - C-590/22, DB 2024, 1676 Rn. 26 – PS GbR; vom 11. April 2024 – C-741/21, NJW 2024, 1561 Rn. 36 – juris; vom 4. Mai 2023 – C-300/21, VersR 2023, 920 Rn. 51 – Österreichische Post). Allerdings hat der Gerichtshof auch erklärt, dass diese Person nach Art. 82 Abs. 1 DSGVO verpflichtet ist, nachzuweisen, dass sie tatsächlich einen materiellen oder immateriellen Schaden erlitten hat. Die Ablehnung einer Erheblichkeitsschwelle 120

bedeutet nicht, dass eine Person, die von einem Verstoß gegen die Datenschutz-Grundverordnung betroffen ist, der für sie negative Folgen gehabt hat, vom Nachweis befreit wäre, dass diese Folgen einen immateriellen Schaden im Sinne von Art. 82 dieser Verordnung darstellen (EuGH, Urteile vom 20. Juni 2024 – C-590/22, DB 2024, 1676 Rn. 27 – PS GbR; vom 11. April 2024 – C-741/21, NJW 2024, 1561 Rn. 36 – ju – ris). Schließlich hat der Gerichtshof in seiner jüngeren Rechtsprechung unter Bezugnahme auf ErwG 85 DSGVO (vgl. ferner ErwG 75 DSGVO) klargestellt, dass schon der – selbst kurzzeitige – Verlust der Kontrolle über personenbezogene Daten einen immateriellen Schaden darstellen kann, ohne dass dieser Begriff des „immateriellen Schadens“ den Nachweis zusätzlicher spürbarer negativer Folgen erfordert (EuGH, Urteile vom 4. Oktober 2024 – C-200/23, juris Rn. 145,156 i.V.m. 137-Agentsia po vpisvaniyata; vom 20. Juni 2024 – C-590/22, DB 2024, 1676 Rn. 33 – PS GbR; vom 11. April 2024 – C-741/21, NJW 2024, 1561 Rn. 42 – juris; vgl. zuvor bereits EuGH, Urteile vom 25. Januar 2024 – C-687/21, CR 2024, 160 Rn. 66 – MediaMarktSaturn; vom 14. Dezember 2023 – C-456/22, NZA 2024, 56 Rn. 17-23 – Gemeinde Ummendorf sowie – C-340/21, NJW 2024, 1091 Rn. 82 – Natsionalna agentsia za prihodite). Im ersten Satz des 85. Erwägungsgrundes der DSGVO heißt es, dass ”[e]ine Verletzung des Schutzes personenbezogener Daten … – wenn nicht rechtzeitig und angemessen reagiert wird – einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen [kann], wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste … oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person“. Aus dieser beispielhaften Aufzählung der „Schäden“, die den betroffenen Personen entstehen können, geht nach der Rechtsprechung des Gerichtshofs hervor, dass der Unionsgesetzgeber unter den Begriff „Schaden“ insbesondere auch den bloßen Verlust der Kontrolle („the mere loss of control“, „la simple perte de contrôle“) über ihre eigenen Daten infolge eines Verstoßes gegen die Datenschutz-Grundverordnung fassen wollte, selbst wenn konkret keine missbräuchliche Verwendung der betreffenden Daten zum Nachteil dieser Personen erfolgt sein sollte (EuGH, Urteile vom 4. Oktober 2024 – C-200/23, juris Rn. 145 – Agentsia po vpisvaniyata; vom 14. Dezember 2023 – C-340/21, NJW 2024,1091 Rn. 82 – Natsionalna agentsia za prihodite). Freilich muss auch insoweit die betroffene Person den Nachweis erbringen, dass sie einen solchen – d.h. in einem bloßen Kontrollverlust als solchem bestehenden – Schaden erlitten hat (vgl. EuGH, Urteile vom 20. Juni 2024 – C-590/22, DB 2024, 1676 Rn. 33 – PS GbR; vom 11. April 2024 – C-741/21, NJW 2024, 1561 Rn. 36 und 42 – juris). Ist dieser Nachweis erbracht, steht der Kontrollverlust also fest, stellt dieser selbst den immateriellen Schaden dar und es bedarf keiner sich daraus entwickelnden besonderen Befürchtungen oder Ängste der betroffenen Person; diese wären lediglich geeignet, den eingetretenen immateriellen Schaden noch zu vertiefen oder zu vergrößern.“

Ein derartiger Schaden in Form eines Kontrollverlustes liegt vorliegend in der hier anzunehmenden Veröffentlichung der Daten der Klägerin im Darknet bzw. im frei zugänglichen Internet. Eine für die Bejahung eines Schadens ausreichende Verletzung des allgemeinen Persönlichkeitsrechts in der Ausprägung des Rechts auf informationelle Selbstbestimmung in Form eines Kontrollverlustes liegt hier vor. Das Recht auf informationelle Selbstbestimmung enthält die Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann, wo und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden. Dieses Recht der Klägerin wurde verletzt. Infolge der obigen Verstöße gegen die einschlägigen Bestimmungen der DSGVO gelangten jedenfalls die im unstreitigen Teil des Tatbestandes aufgeführten Daten auf jedenfalls eine online betriebene Seite im Darknet, auf der sie über einen erheblichen Zeitraum rechtswidrig und massenhaft zum weiteren Vertrieb angeboten werden. Hierdurch wurde das dargelegte Recht der Klägerin 121

verletzt, selbst zu entscheiden, wo und ob sie diese Daten offenbaren möchte. Hierin liegt ein von der DSGVO-Verletzung selbst zu trennender Datenabfluss ins Darknet samt dortiger Weiterverarbeitung und Veröffentlichung durch illegal handelnde Dritte, der tatsächlich passiert ist und damit zu einer konkreten und individuell benennbaren Verletzung des Rechts der Klägerin auf informationelle Selbstbestimmung gekommen ist (vgl. LG Lübeck, Urteil vom 04.10.2024 – 15 O 216/23, GRUR-RS 2024, 26215, Rn. 99, 102).

Bei der Bemessung des dafür ersatzfähigen Schadens hält das Gericht den tenorierten Betrag in Höhe von 100,- € für angemessen und ausreichend. Es lehnt sich dabei an die Hinweise des BGH im Grundsatzurteil zum Scraping bei Facebook an, wo grundsätzlich wie folgt ausgeführt worden ist: 122

„In Anbetracht der Ausgleichsfunktion des in Art. 82 DSGVO vorgesehenen Schadenersatzanspruchs, wie sie in Erwgr. 146 S. 6 DSGVO zum Ausdruck kommt, ist eine auf Art. 82 DS-GVO gestützte Entschädigung in Geld als „vollständig und wirksam“ anzusehen, wenn sie es ermöglicht, den aufgrund des Verstoßes gegen diese Verordnung konkret erlittenen Schaden in vollem Umfang auszugleichen; eine Abschreckungs- oder Straffunktion soll der Anspruch aus Art. 82 I DSGVO dagegen nicht erfüllen (vgl. EuGH GRUR-RS 2024, 13978 Rn. 42 = DB 2024, 1676 – PS GbR; vgl. auch EuGH GRUR 2024, 1838 Rn. 43 f. – Pat?r?t?ju ties?bu aizsardz?bas centrs; EuGH NJW 2024, 2599 = GRUR-RS 2024, 13981 Rn. 23 – Scalable Capital; EuGH GRUR 2024, 784 Rn. 59 = NJW 2024, 1561 – juris; EuGH GRUR-RS 2024, 530 Rn. 47 = CR 2024, 160 – MediaMarktSaturn). Folglich darf weder die Schwere des Verstoßes gegen die Datenschutz-Grundverordnung, durch den der betreffende Schaden entstanden ist, berücksichtigt werden, noch der Umstand, ob ein Verantwortlicher mehrere Verstöße gegenüber derselben Person begangen (EuGH GRUR 2024, 784 Rn. 60 u. 64 f. = NJW 2024, 1561 – juris) und ob er vorsätzlich gehandelt hat (EuGH NJW 2024, 2599 = GRUR-RS 2024, 13981 Rn. 29 f. – Scalable Capital). 123

Im Ergebnis soll die Höhe der Entschädigung zwar nicht hinter dem vollständigen Ausgleich des Schadens zurückbleiben, sie darf aber auch nicht in einer Höhe bemessen werden, die über den vollständigen Ersatz des Schadens hinausginge (vgl. EuGH GRUR 2024, 784 Rn. 60 = NJW 2024, 1561 – juris; EuGH GRUR-RS 2024, 530 Rn. 48 = CR 2024, 160 – MediaMarktSaturn). Ist der Schaden gering, ist daher auch ein Schadensersatz in nur geringer Höhe zuzusprechen (vgl. EuGH GRUR 2024, 1838 Rn. 35 – Pat?r?t?ju ties?bu aizsardz?bas centrs; EuGH NJW 2024, 2599 = GRUR-RS 2024, 13981 Rn. 45 f. – Scalable Capital). 124

Dies gilt auch unter Berücksichtigung des Umstands, dass der durch eine Verletzung des Schutzes personenbezogener Daten verursachte immaterielle Schaden seiner Natur nach nicht weniger schwerwiegend ist als eine Körperverletzung (vgl. dazu EuGH ECLI:EU:C:2024:827 = GRUR-RS 2024, 26255 Rn. 151 – Agentsia po vpisvaniyata; EuGH NJW 2024, 2599 = GRUR-RS 2024, 13981 Rn. 39 – Scalable Capital). 125

(…) 126

Ist nach den Feststellungen des Gerichts allein ein Schaden in Form eines Kontrollverlusts an personenbezogenen Daten gegeben, weil weitere Schäden nicht nachgewiesen sind, hat der Tatrichter bei der Schätzung des Schadens insbesondere die etwaige Sensibilität der konkret betroffenen personenbezogenen Daten (vgl. Art. 9 I DSGVO) und deren typischerweise zweckgemäße Verwendung zu berücksichtigen. Weiter hat er die Art des Kontrollverlusts (begrenzter/unbegrenzter Empfängerkreis), die Dauer des Kontrollverlusts und die Möglichkeit der Wiedererlangung der Kontrolle etwa durch Entfernung einer Veröffentlichung 127

aus dem Internet (inkl. Archiven) oder Änderung des personenbezogenen Datums (zB Rufnummernwechsel; neue Kreditkartennummer) in den Blick zu nehmen. Als Anhalt für einen noch effektiven Ausgleich könnte in den Fällen, in denen die Wiedererlangung der Kontrolle mit verhältnismäßigem Aufwand möglich wäre, etwa der hypothetische Aufwand für die Wiedererlangung der Kontrolle (hier insbesondere eines Rufnummernwechsels) dienen.

Äußerst zweifelhaft erscheint daher, ob hier eine Festsetzung in „gegebenenfalls nur einstelliger Höhe“ mit dem Effektivitätsgrundsatz zu vereinbaren wäre (so aber obiter OLG Celle 4.4.2024 – 5 U 31/23, GRUR-RS 2024, 6435, juris-Rn. 102). Dagegen hätte der Senat von Rechts wegen keine Bedenken, den notwendigen Ausgleich für den eingetretenen Kontrollverlust als solchem in einem Fall wie dem streitgegenständlichen in einer Größenordnung von 100 EUR (so obiter OLG Hamm 21.6.2024 – 7 U 154/23, GRUR-RS 2024, 16856, juris-Rn. 40) zu bemessen.“ 128

(BGH, Urteil vom 18. November 2024 - VI ZR 10/24, Rn. 96 ff.) 129

Nach diesen Grundsätzen ist zunächst festzustellen, dass die betroffenen Daten maßgeblich den Vor- und Nachnamen, die E-Mail Adresse und das Geburtsdatum enthalten. Dabei handelt es sich nicht um sensible Daten gem. Art. 9 Abs. 1 DSGVO. Diese Daten sind auch regelmäßig notwendig, um Dienste und Leistungen im Internet wahrzunehmen, da insoweit ein elektronischer Kommunikationsweg geschaffen wird, die Identität der Person klargestellt und ihr Alter etwa zur Prüfung der Volljährigkeit angegeben wird. Dabei ist jedoch die Verbindung von Klarnamen, Geburtsdatum und E-Mail Adresse durchaus geeignet, Missbrauch zu begünstigen. 130

Hinzu kommt, dass diese Daten einem potentiell unbegrenzten Empfängerkreis für eine nicht unerhebliche Zeit zur Verfügung standen. Die Möglichkeit zur Wiedererlangung der Kontrolle über die eigenen Daten besteht faktisch nur darin, die E-Mail Adresse zu ändern – Name und Geburtsdatum sind ersichtlich nicht zu ändern. Kosten werden für einen Wechsel der E-Mail Adresse regelmäßig nicht anfallen, jedoch ein nicht unerheblicher Aufwand, um die neue E-Mail Adresse bei allen Kontakten bekannt zu machen und bei allen genutzten Internet-Diensten etc. zu hinterlegen. 131

Unter Beachtung dieser Aspekte handelt es sich nicht um einen Bagatellfall, jedoch auch nicht um einen außergewöhnlichen Fall. Die vom BGH im Scraping-Komplex bei Facebook in den Raum gestellten 100,- € erscheinen demnach auch hier als angemessener Betrag. Dabei hat das Gericht auch beachtet, dass die E-Mail Adresse (und damit faktisch auch der darin enthaltene Klarname der Klägerin) ausweislich der auch von ihr selbst zur Darlegung ihrer Betroffenheit angeführten Internetseite www.entfernt.com bei insgesamt fünf und neben dem hier gegenständlichen bei vier weiteren angeblichen Datenschutzvorfällen betroffen sein soll. Dies ist in der Gesamtschau jedenfalls kein Grund, den vom BGH vorgeschlagenen Schadensbetrag für den „reinen Kontrollverlust“ nach oben hin anzupassen. Denn dieser Kontrollverlust der Klägerin an ihren Daten beruht nach eigenem Vorbringen nicht ausschließlich auf dem DSGVO-Verstoß der Beklagten, sondern fußt auf mehreren Beinen. 132

bb) Eine höhere immaterielle Entschädigung war nicht aufgrund von individuellen psychischen Beeinträchtigungen der Klägerin durch den Datenschutz-Vorfall geboten. 133

Unabhängig vom Nachweis eines Kontrollverlusts reicht für einen Anspruch auf einen immateriellen Schadensersatz zwar auch die begründete Befürchtung einer Person, dass ihre personenbezogenen Daten aufgrund eines Verstoßes gegen die Verordnung von Dritten missbräuchlich verwendet werden, aus, um einen Schadensersatzanspruch zu begründen 134

(vgl. EuGH, Urteil vom 25. Januar 2024 – C-687/21, CR 2024, 160 Rn. 67 – MediaMarktSaturn; vom 14. Dezember 2023 – C-340/21, NJW 2024, 1091 Rn. 85 – Natsionalna agentsia za prihodite). Die Befürchtung samt ihrer negativen Folgen muss dabei ordnungsgemäß nachgewiesen sein (vgl. EuGH, Urteile vom 20. Juni 2024 – C-590/22, DB 2024,1676 Rn. 36 – PS GbR; vom 14. Dezember 2023 – C-340/21, NJW 2024, 1091 Rn. 75-86 – Natsionalna agentsia za prihodite). Demgegenüber genügt die bloße Behauptung einer Befürchtung ohne nachgewiesene negative Folgen ebenso wenig wie ein rein hypothetisches Risiko der missbräuchlichen Verwendung durch einen unbefugten Dritten (vgl. EuGH, Urteile vom 20. Juni 2024 – C-590/22, DB 2024, 1676 Rn. 35 – PS GbR; vom 25. Januar 2024 – C-687/21, CR 2024, 160 Rn. 68 – MediaMarktSaturn). Sind derartige psychische Beeinträchtigungen infolge einer Anhörung des Betroffenen nachgewiesen, ist der Entschädigungsbetrag in einer Höhe festzusetzen, die über dem im Falle eines bloßen Kontrollverlustes zuzusprechenden Betrag liegt (BGH, Urteil vom 18.11.2024 – Rn VIII 2 c) cc); zitiert nach OLG Dresden, Endurteil vom 10.12.2024 – 4 U 808/24, GRUR-RS 2024, 35688, Rn. 21).

Einer informatorischen Anhörung der Klägerin bedurfte es vorliegend aber auch im Lichte des BGH-Urteils in Sachen Scraping bei Facebook nicht. Der BGH führte dort aus, dass für den Fall, dass der Betroffene psychische Beeinträchtigungen geltend macht, die über die mit dem eingetretenen Kontrollverlust für jedermann unmittelbar zusammenhängenden Unannehmlichkeiten hinausgehen, das Tatgericht gegebenenfalls gehalten ist, den Betroffenen anzuhören, um die notwendigen Feststellungen hierzu treffen zu können (BGH, Urteil vom 18. November 2024 - VI ZR 10/24, Rn. 101). Das Gericht erkennt gerade dies vorliegend nicht. Vielmehr macht die Klägerin – wie aus der Erfahrung des Gerichts aus einer großen Vielzahl gleichgelagerter Fälle in verschiedenen DSGVO-Fällen mit verschiedenen Beklagtenparteien – genau dieselben Folgen der Veröffentlichung ihrer Daten im Darknet bzw. Internet geltend. Namentlich wird eine erhöhtes Spam-Aufkommen und die Sorge vor Phishing vorgetragen. Dies ist aber gerade die naheliegende und unmittelbare Folge des Kontrollverlustes und keine eigenständige Schadensposition. Diese Aspekte sind bereits in dem oben geschätzten Schaden enthalten. Eine Erhöhung ist schon deshalb nicht geboten, weil die Klägerin offenbar nunmehr für das Thema sensibilisiert ist und nicht allzu einfach Opfer einer Phishing Attacke werden dürfte. Im Übrigen könnte sie sich, auch wenn dies aufwändig erscheint, durch einen Wechsel ihrer E-Mail Adresse den Phishing Angriffen entziehen. 135

Im Übrigen bleibt der Sachvortrag derart pauschal und ist dem aus anderen Fällen der Prozessbevollmächtigten der Klägerin wortgleich bekannt, dass eine Anhörung der Klägerin hierzu nicht geboten war. Die informatorische Anhörung der Partei ersetzt nicht einen substantiierten Parteivortrag. Dies zeigt sich exemplarisch an der Behauptung, dass die Klägerin „aufgrund des Datenlecks und deren Auswirkungen aufgrund von Angstzuständen in ärztlicher Behandlung“ sei und „gelegentlich Schlafstörungen“ aufgetreten seien. Insbesondere wird eine angebliche ärztliche Behandlung nicht durch ein Attest o.Ä. substantiiert. 136

Mit Blick auf den übrigen Sachvortrag der Klägerin ist eine konkrete emotionale Beeinträchtigung der Klägerin nicht ersichtlich. Die schriftsätzlich allgemein gehaltenen Behauptungen der Klägerin zu Sorgen und Ängsten über einen möglichen Missbrauch gehen über alltägliche Empfindungen, die keine begründete Befürchtung rechtfertigen, nicht hinaus. Den Schluss auf einen realen und sicheren emotionalen Schaden (vgl. Schlussanträge des Generalanwaltes D. vom 27.04.2023 – C -340/21, Rn 82, 83, – juris) erlauben sie nicht. Da im Allgemeinen jeder Verstoß gegen eine Norm über den Schutz personenbezogener Daten zu 137

einer negativen Reaktion der betroffenen Person führen kann (vgl. Schlussanträge des Generalanwaltes W. C.-A. von 06.10.2022 – C 300/21, Rn 113 – juris) und ein Schadensersatz, der sich aus einem bloßen Unmutsgefühl wegen der Nichtbeachtung des Rechts durch einen anderen ergibt, einem „Schadensersatz ohne Schaden“ recht nahe kommt, der nicht von Art. 82 erfasst ist (vgl. EuGH, Urteil vom 04.05.2023 – C – 300/21, Rn. 36 ff – juris), reicht demgegenüber allein die bloße Beunruhigung wegen des Diebstahls der eigenen personenbezogenen Daten nicht aus (vgl. Schlussanträge des Generalanwaltes S. vom 26.10.2023 – C 182/22, Rn 24 – juris / vgl. OLG Dresden, Endurteil vom 10.12.2024 – 4 U 808/24, GRUR-RS 2024, 35688, Rn. 22).

cc) Die Kausalität im Sinne einer „haftungsausfüllenden Kausalität“ – sofern erforderlich – ist ebenfalls gegeben. Der festgestellte Schaden beruht kausal auf dem oben festgestellten Verstoß gegen die DSGVO und zwar sowohl äquivalent als auch adäquat kausal. Bei Beachtung der Pflichten im Zuge der Beendigung der Zusammenarbeit mit der P. Inc. wäre es nicht zum hier gegenständlichen Kontrollverlust der Daten der Klägerin gekommen. 138

An dieser Stelle steht der Kausalität nicht entgegen, dass nach dem eigenen klägerischen Vortrag ihre E-Mail Adresse laut der Webseite entfernt.com von vier weiteren Datenschutzvorfällen betroffen sein soll. Dass diese Datenschutzvorfälle tatsächlich stattgefunden haben und die Klägerin davon betroffen ist, wird von keiner der Parteien substantiiert dargelegt. Insbesondere wird aber von der Beklagten nicht gem. Art. 82 Abs. 3 DSGVO nachgewiesen, dass anderweitige Datenschutzvorfälle bereits zu einem Kontrollverlust geführt hätten. 139

g) Der Ausspruch zur Verzugsverzinsung folgt aus §§ 291, 288 Abs. 1 BGB. 140

2. Klageantrag zu 2) – Feststellung 141

Angesichts der obigen Ausführungen und im Anschluss an das oben bereits zitierte Urteil des BGH vom 18.11.2024 steht der Klägerin auch ein Anspruch auf Feststellung der Verpflichtung der Beklagten, alle künftigen (materiellen) Schäden zu erstatten, zu. 142

Der BGH hat hierzu ausgeführt, die Möglichkeit des Eintritts künftiger Schäden sei ohne Weiteres zu bejahen, wenn die Klagepartei – wie hier – durch einen Verstoß gegen die Datenschutz-Grundverordnung in ihrem Recht auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG bzw. auf Schutz der personenbezogenen Daten gemäß Art. 8 GRCh verletzt worden sei und durch die fortdauernde Veröffentlichung ihrer personenbezogenen Daten (insbesondere ihres Namens in Verbindung mit ihrer Telefonnummer) das Risiko einer missbräuchlichen, insbesondere betrügerischen Nutzung dieser Daten mit der Folge eines materiellen oder immateriellen Schadens fortbestehe. In Anbetracht des hier zu unterstellenden bereits eingetretenen und noch andauernden Kontrollverlusts über diese Daten sei eine künftige Schadensentwicklung auch nicht nur rein theoretischer Natur. So liegt es auch hier. Angesichts des feststehenden Verstoßes der Beklagten gegen ihre datenschutzrechtlichen Pflichten, ist der Feststellungsanspruch auch der Sache nach begründet (vgl. OLG Dresden, Endurteil vom 10.12.2024 – 4 U 808/24, GRUR-RS 2024, 35688, Rn. 23). 143

Soweit der Antrag sich auch auf künftige immaterielle Schäden bezieht, so war dies im Wege der Auslegung dahingehend im Tenor klarzustellen, dass hiermit künftige, derzeit noch nicht vorhersehbare immaterielle Schäden erfasst sein sollen, die nicht Gegenstand des Klageantrags zu 1) waren. 144

145

3. Klageantrag zu 3) – weiterer immaterieller Schadensersatz wegen verzögerter Auskunft

Die Klägerin hat keinen Anspruch auf Zahlung eines immateriellen Schadensersatzes aus Art. 82 DSGVO wegen angeblich verzögerter Auskunft. Ein solcher mit dem Klageantrag zu 3) geltend gemachter Anspruch folgt auch aus keinem anderen Rechtsgrund. 146

Ein Anspruch besteht schon deshalb nicht, weil die Auskunftspflicht nach Art. 15 DSGVO – wie nachfolgend auszuführen sein wird – nicht verletzt wurde. Im Übrigen ist nicht ersichtlich, welcher Schaden der Klägerin aus einer möglichen Verletzung der Auskunftspflicht erwachsen könnte. Selbst wenn die Auskunft zu spät erteilt worden wäre, so kann dies offensichtlich weder kausal für den oben allein als Schaden festgestellten Kontrollverlust sein, noch kann dies einen solchen Kontrollverlust verstärken. 147

4. Klageantrag zu 4) – Auskunft 148

Die Klägerin hat keinen Anspruch auf Auskunft nach Art. 15 DSGVO zu, weil der Anspruch von der Beklagten erfüllt worden ist gem. § 362 BGB. 149

Nach Art. 15 Abs. 1 DSGVO hat die betroffene Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und bestimmte weitere Informationen. Gemäß Art. 15 Abs. 3 Satz 1 DSGVO stellt der Verantwortliche eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung (vgl. OLG Hamm im Urteil vom 15.08.2023 – 7 U 19/23, Rn 244 ff. – juris). Erfüllt im Sinne des § 362 Abs. 1 BGB ist ein Auskunftsanspruch grundsätzlich dann, wenn die Angaben nach dem erklärten Willen des Schuldners die Auskunft im geschuldeten Gesamtumfang darstellen. Wird die Auskunft in dieser Form erteilt, steht ihre etwaige inhaltliche Unrichtigkeit einer Erfüllung nicht entgegen. Der Verdacht, dass die erteilte Auskunft unvollständig oder unrichtig ist, kann einen Anspruch auf Auskunft in weitergehendem Umfang nicht begründen. Wesentlich für die Erfüllung des Auskunftsanspruchs ist daher die – gegebenenfalls konkludente – Erklärung des Auskunftsschuldners, dass die Auskunft vollständig ist. Die Annahme eines derartigen Erklärungsinhalts setzt demnach voraus, dass die erteilte Auskunft erkennbar den Gegenstand des berechtigten Auskunftsbegehrens vollständig abdecken soll. Daran fehlt es beispielsweise dann, wenn sich der Auskunftspflichtige hinsichtlich einer bestimmten Kategorie von Auskunftsgegenständen nicht erklärt hat, etwa weil er irrigerweise davon ausgeht, er sei hinsichtlich dieser Gegenstände nicht zur Auskunft verpflichtet. Dann kann der Auskunftsberechtigte eine Ergänzung der Auskunft verlangen (vgl. BGH Urt. v. 15.6.2021 – VI ZR 576/19, – juris / zitiert nach OLG Dresden, Urteil vom 15.10.2024 – 4 U 422/24, GRUR-RS 2024, 29008, Rn. 60). 150

Die Beklagte hat der Klägerin die Liste der Empfänger der Daten und einen Auszug der personenbezogenen Daten, die über sie gehalten werden, vorgerichtlich mitgeteilt (Anlage B14 – die von der Klägerin in der Klageschrift aus unerfindlichen Gründen nicht vorgelegt worden ist, was das Gericht als Prozessverhalten als unangemessen ansieht). In der Klageerwiderung hat die Beklagte ebenfalls Auskunft durch Vorlage der Anlage B6 erteilt. Darüber hinaus hat die Beklagte auf ihrer Webseite ihre Nutzer über den Datenvorfall und über die Art der Daten, die davon betroffen sind (z.B.: Vor- und Nachname und e-mail Adresse) informiert (Anlage B 8). Eine weitere Information der Nutzer über den Cyberangriff bei dem früheren Dienstleister erfolgte am 31.01.2023 (Anlage B 9). Damit ist die Beklagte ihren Pflichten in ausreichendem Umfang nachgekommen. 151

152

Soweit die Klagepartei Auskunft darüber verlangt, welche Daten, wann durch welche Personen erlangt wurden, so steht dem Anspruch § 275 Abs. 1 BGB entgegen. Insofern weist die Beklagte unwidersprochen darauf hin, dass ihr die Identitäten der Hacker nicht bekannt ist. Eine Auskunftserteilung ist ihr daher unmöglich.

5. Klageantrag zu 6) – vorgerichtliche Rechtsanwaltsgebühren 153

Ausgehend von dem Obsiegen der Klägerin in diesem Verfahren besteht ein Anspruch auf Erstattung vorgerichtlicher Rechtsanwaltskosten lediglich in der aus dem Tenor ersichtlichen Höhe. 154

Die Kosten der Rechtsverfolgung und deshalb auch die Kosten eines mit der Sache befassten Rechtsanwalts gehören nach der ständigen Rechtsprechung des BGH, soweit sie zur Wahrnehmung der Rechte erforderlich und zweckmäßig waren, grundsätzlich zu dem wegen einer unerlaubten Handlung zu ersetzenden Schaden (vgl. BGH, Urteile vom 17. November 2015 – VI ZR 492/14, NJW 2016, 1245 Rn. 9; vom 4. März 2008 – VI ZR 176/07, VersR 2008, 985 Rn. 5; vom 4. Dezember 2007 – VI ZR 277/06, VersR 2008, 413 Rn. 13; vom 8. November 1994 – VI ZR 3/94, BGHZ 127, 348, 350, juris Rn. 7). Dabei ist maßgeblich, wie sich die voraussichtliche Abwicklung des Schadensfalls aus der Sicht des Geschädigten darstellt. Ist die Verantwortlichkeit für den Schaden und damit die Haftung von vornherein nach Grund und Höhe derart klar, dass aus der Sicht des Geschädigten kein vernünftiger Zweifel daran bestehen kann, dass der Schädiger ohne weiteres seiner Ersatzpflicht nachkommen werde, so wird es grundsätzlich nicht erforderlich sein, schon für die erstmalige Geltendmachung des Schadens gegenüber dem Schädiger einen Rechtsanwalt hinzuzuziehen. In derart einfach gelagerten Fällen kann der Geschädigte grundsätzlich den Schaden selbst geltend machen, so dass sich die sofortige Einschaltung eines Rechtsanwalts nur unter besonderen Voraussetzungen als erforderlich erweisen kann, wenn etwa der Geschädigte aus Mangel an geschäftlicher Gewandtheit oder sonstigen Gründen wie etwa Krankheit oder Abwesenheit nicht in der Lage ist, den Schaden selbst anzumelden (vgl. BGH, Urteil vom 8. November 1994 – VI ZR 3/94, BGHZ 127, 348, 351 f juris Rn. 9). Ein solcher Fall liegt hier indes nicht vor, die Einschaltung eines Rechtsanwalts war hier wegen der ablehnenden Haltung der Beklagten gerechtfertigt (vgl. insgesamt zum vorstehenden Absatz: OLG Dresden, Endurteil v. 10.12.2024 – 4 U 808/24, GRUR-RS 2024, 35688, Rn. 35). Dies gilt auch für die Geltendmachung des im Nachgang erfüllten Auskunftsbegehrens. 155

Nach diesen Maßstäben kann ein materiell-rechtlicher Kostenerstattungsanspruch aus Art. 82 Abs. 1 DSGVO für die anwaltliche Tätigkeit in Fallgestaltungen des Scraping-Komplexes im Grundsatz nicht verneint werden (BGH, Urteil vom 18.11.2024 – VI ZR 10/24). Dies gilt auch im vorliegenden Fall. Der Höhe nach besteht ein solcher Anspruch jedoch lediglich für die Geltendmachung einer 1,3-Geschäftsgebühr nach Nr. 2300 KV RVG aus einem Streitwert von 1.100,- € (100 € immaterieller Schaden + 500 € Feststellung + 500 € Auskunft), also 165,10 €, zuzüglich Postpauschale iHv 20 € und USt. iHv 35,17 €, mithin insgesamt 220,27 €. 156

Der Ausspruch zur Verzugsverzinsung folgt aus §§ 291, 288 Abs. 1 BGB. 157

III. Es bestand kein Anlass die mündliche Verhandlung wieder zu eröffnen. Insbesondere war die Änderung eines Teils der Klageanträge nach der mündlichen Verhandlung kein Grund, die mündliche Verhandlung wieder zu eröffnen (s.o.). Auch hat die Klägerin in der Spruchfrist keinen neuen entscheidungserheblichen Sachvortrag eingeführt, der eine Wiedereröffnung der mündlichen Verhandlung notwendig gemacht hätte. Das Gericht hat die beiderseits eingereichten, nicht nachgelassenen Schriftsätze zur Kenntnis genommen und zum 158

Gegenstand seiner Entscheidungsfindung gemacht.

IV. Die Kostenentscheidung beruht auf § 92 Abs. 2 Nr. 1 ZPO. Die Klägerin obsiegt im Verhältnis zum Gesamtstreitwert nur mit einem Anteil von 8%, wobei der Klageantrag zu 6) als Nebenforderung außer Acht geblieben ist. Es entspricht der ständigen Rechtsprechung des Einzelrichters, bei einem Obsiegen mit weniger als 1/10 des Gesamtstreitwerts die Kosten insgesamt der weitgehend unterlegenen Partei aufzuerlegen. Davon war hier keine Ausnahme zu machen. 159

Der Ausspruch zur vorläufigen Vollstreckbarkeit beruht auf § 708 Nr. 11, 711 ZPO. 160

V. Der Streitwert wird auf 7.500,00 EUR festgesetzt. 161

Justiz NRW
Rechtsprechungsdatenbank ONLINE