



BUNDESGERICHTSHOF

BESCHLUSS

VI ZR 258/24

vom

28. August 2025

in dem Rechtsstreit

Nachschlagewerk: ja

BGHZ: nein

BGHR: ja

JNEU: ja

Verordnung (EU) 2016/679 Art. 82 Abs. 1

Dem Gerichtshof der Europäischen Union werden zur Auslegung der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, DSGVO, ABl. L 119 vom 4. Mai 2016, S. 1) folgende Fragen zur Vorabentscheidung vorgelegt:

a) Ist Art. 4 Nr. 1 DSGVO dahingehend auszulegen, dass im Falle der automatisierten Übermittlung einer dynamischen Internetprotokoll-Adresse (IP-Adresse) diese bereits dann ein personenbezogenes Datum darstellt, wenn ein Dritter über das zur Identifizierung der betroffenen Person erforderliche Zusatzwissen verfügt?

Oder ist Voraussetzung für die Annahme eines personenbezogenen Datums, dass der für die Übermittlung Verantwortliche oder der Empfänger über Mittel verfügen, die vernünftigerweise eingesetzt werden können, die betreffende Person - gegebenenfalls mit Hilfe eines Dritten - bestimmen zu lassen?

ECLI:DE:BGH:2025:280825BVIZR258.24.0

Falls letzteres zutrifft: Genügt es insoweit, dass unter bestimmten Voraussetzungen rechtliche Möglichkeiten zur Identifizierung der betroffenen Person bestehen können oder müssen diese Voraussetzungen in tatsächlicher und rechtlicher Sicht im konkreten Fall vorgelegen haben?

- b) Ist Art. 82 Abs. 1 DSGVO dahingehend auszulegen, dass ein immaterieller Schaden auch dann vorliegen kann, wenn die betroffene Person einen Verstoß des Verantwortlichen gegen die Datenschutz-Grundverordnung bewusst und allein zu dem Zweck herbeiführt, den Verstoß dokumentieren und gegenüber dem Verantwortlichen geltend machen zu können?

Falls ja: Kann das Vorliegen eines immateriellen Schadens auch dann bejaht werden, wenn gleichartige Verstöße in großer Zahl in automatisierter Weise provoziert werden?

- c) Falls beide unter Ziffer 2 aufgeworfenen Fragen bejaht werden:

Ist Art. 82 Abs. 1 DSGVO dahingehend auszulegen, dass in einem Fall der in Frage 2 beschriebenen Art ein Anspruch auf Ersatz immateriellen Schadens wegen missbräuchlichen Verhaltens der betroffenen Person verneint werden kann, weil trotz formaler Einhaltung der in der Unionsregelung vorgesehenen Bedingungen das Ziel dieser Regelung nicht erreicht wurde und die Absicht bestand, sich einen aus der Unionsregelung resultierenden Vorteil zu verschaffen, indem die Voraussetzungen für seine Erlangung künstlich geschaffen werden? Kommt es insoweit darauf an, ob die Erlangung eines finanziellen Vorteils die alleinige Motivation für die Provokation des Verstoßes gegen die Verordnung war?

BGH, Beschluss vom 28. August 2025 - VI ZR 258/24 - LG Hannover
AG Hannover

Der VI. Zivilsenat des Bundesgerichtshofs hat auf die mündliche Verhandlung vom 27. Mai 2025 durch die Richterin von Pentz als Vorsitzende, die Richterin Dr. Oehler, die Richter Dr. Allgayer und Böhm sowie die Richterin Dr. Linder beschlossen:

- I. Das Verfahren wird ausgesetzt.
- II. Dem Gerichtshof der Europäischen Union werden zur Auslegung der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, DSGVO, ABl. L 119 vom 4. Mai 2016, S. 1) folgende Fragen zur Vorabentscheidung vorgelegt:
 1. Ist Art. 4 Nr. 1 DSGVO dahingehend auszulegen, dass im Falle der automatisierten Übermittlung einer dynamischen Internetprotokoll-Adresse (IP-Adresse) diese bereits dann ein personenbezogenes Datum darstellt, wenn ein Dritter über das zur Identifizierung der betroffenen Person erforderliche Zusatzwissen verfügt?

Oder ist Voraussetzung für die Annahme eines personenbezogenen Datums, dass der für die Übermittlung Verantwortliche oder der Empfänger über Mittel verfügen, die vernünftigerweise eingesetzt werden können, die betreffende Person - gegebenenfalls mit Hilfe eines Dritten - bestimmen zu lassen?

Falls letzteres zutrifft: Genügt es insoweit, dass unter bestimmten Voraussetzungen rechtliche Möglichkeiten zur Identifizierung

der betroffenen Person bestehen können oder müssen diese Voraussetzungen in tatsächlicher und rechtlicher Sicht im konkreten Fall vorgelegen haben?

2. Ist Art. 82 Abs. 1 DSGVO dahingehend auszulegen, dass ein immaterieller Schaden auch dann vorliegen kann, wenn die betroffene Person einen Verstoß des Verantwortlichen gegen die Datenschutz-Grundverordnung bewusst und allein zu dem Zweck herbeiführt, den Verstoß dokumentieren und gegenüber dem Verantwortlichen geltend machen zu können?

Falls ja: Kann das Vorliegen eines immateriellen Schadens auch dann bejaht werden, wenn gleichartige Verstöße in großer Zahl in automatisierter Weise provoziert werden?

3. Falls beide unter Ziffer 2 aufgeworfenen Fragen bejaht werden:

Ist Art. 82 Abs. 1 DSGVO dahingehend auszulegen, dass in einem Fall der in Frage 2 beschriebenen Art ein Anspruch auf Ersatz immateriellen Schadens wegen missbräuchlichen Verhaltens der betroffenen Person verneint werden kann, weil trotz formaler Einhaltung der in der Unionsregelung vorgesehenen Bedingungen das Ziel dieser Regelung nicht erreicht wurde und die Absicht bestand, sich einen aus der Unionsregelung resultierenden Vorteil zu verschaffen, indem die Voraussetzungen für seine Erlangung künstlich geschaffen werden? Kommt es insoweit darauf an, ob die Erlangung eines finanziellen Vorteils die alleinige Motivation für die Provokation des Verstoßes gegen die Verordnung war?

Gründe:

1 A. Sachverhalt und Ausgangsrechtsstreit

2 Der Kläger verlangt von den Beklagten die Rückerstattung eines Betrages, den er an den Beklagten zu 1 im Hinblick auf einen von den Beklagten geltend gemachten angeblichen Verstoß gegen die Datenschutz-Grundverordnung (DSGVO) gezahlt hat.

3 Der Kläger betreibt eine Website, auf der er Google Fonts eingebunden hatte. Google Fonts ist ein Verzeichnis mit über 1.500 Schriftarten, das Google den Betreibern von Webseiten zur kostenlosen Verwendung bereitstellt. Mit dem Aufruf einer Domain über einen Browser baut sich die aufgerufene Website unter Nutzung der benötigten Fonts auf. Dadurch werden bei einem Besuch der jeweiligen Webseiten - soweit die Voreinstellung einer dynamischen Einbindung vom Webseitenbetreiber nicht geändert wurde - die Schriften von Google Fonts über einen Google-Server nachgeladen und die jeweilige IP-Adresse des Besuchers an Google in den USA übermittelt. Eine Anpassung der Einstellungen ermöglicht es dem Webseitenbetreiber, die Schriftarten nur lokal einzubinden, so dass die Datenübermittlung in die USA ausbleibt. Diese Anpassung hatte der Kläger nicht vorgenommen.

4 Der Beklagte zu 1 benutzte einen sogenannten Webcrawler, also eine spezifisch hierfür programmierte Computersoftware, um automatisiert eine Vielzahl von Webseiten auf die dynamische Einbindung von Google Fonts zu überprüfen. Dieser Webcrawler war auf dem Laptop des Beklagten zu 1 eingerichtet. Unter anderem bei der Website des Klägers erzielte er so einen "Treffer". Unter Zuhilfenahme einer weiteren extra dafür entwickelten Software wurde ein Besuch des Beklagten zu 1 auf der Website des Klägers automatisiert vorgenommen.

Die dabei an den Beklagten zu 1 vergebene dynamische IP-Adresse wurde an Google USA weitergeleitet.

5 Im Oktober 2022 erhielt der Kläger ein Schreiben des Beklagten zu 2, der dieses in seiner Funktion als Rechtsanwalt namens und in Vollmacht seines Mandanten, des Beklagten zu 1, verfasst hatte. Das Schreiben, das in der Betreffzeile den Begriff "Abmahnung" enthielt, lautete auszugsweise wie folgt:

"Unsere Mandantschaft ist Teil der Interessengemeinschaft Datenschutz; kurz: IG Datenschutz [...]. Die IG Datenschutz hat sich der Verteidigung und Durchsetzung des Datenschutzes auf zivilrechtlichem Weg verschrieben. Der IG Datenschutz ist aufgefallen, dass Sie auf Ihrer Webseite Google Fonts verwenden. Google Fonts ist auf Ihrer Webseite derart installiert, dass unter anderem die IP-Adresse des Besuchers Ihrer Webseite an Google in den USA weitergeleitet wird. Dieser Vorgang wurde auf Bitten unserer Mandantschaft mit ihrer IP-Adresse technisch, wie anliegend dargestellt, gesichert, wobei sich die Weiterleitung an Google aus dem hervorgehobenen Link bestätigt.

Die unerlaubte Weitergabe der IP-Adresse durch Sie an Google stellt eine Verletzung des allgemeinen Persönlichkeitsrechts unserer Mandantschaft in Form des informationellen Selbstbestimmungsrechts nach § 823 Absatz 1 BGB dar. Eine IP-Adresse ist eine personenbezogene Date im Sinne von Art. 4 Nr. 1 DSGVO [...]. Das Recht auf informationelle Selbstbestimmung beinhaltet das Recht des Einzelnen, über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.

Unsere Mandantschaft hat in den Eingriff nicht gemäß Art. 6 Abs. 1 a) DSGVO eingewilligt. Ein Rechtfertigungsgrund für den Eingriff i.S.d. Art. 5 Abs. 1 f) DSGVO liegt nicht vor. Google Fonts kann auch ohne den Aufbau einer Verbindung zum Google Server genutzt werden, womit eine Übertragung der IP-Adresse an Google ausgeschlossen ist.

Aufgrund des Verstoßes hat unsere Mandantschaft gegen Sie u.a. einen Anspruch auf Unterlassung. Deutsche Gerichte haben in den

letzten zwei Jahren Betroffenen von unterschiedlichsten Datenschutzverstößen Schmerzensgelder in einer Breite bis zu einem Maximum von 2.500,00 € zugesprochen [...].

Unsere Mandantschaft ist im Falle der unverzüglichen Beendigung des Verstoßes und Zahlung eines Betrages in Höhe von 170,00 € auf unser Treuhand-Mandanten-Konto [...] bis zum 03.11.2022 bereit, die Sache auf sich beruhen zu lassen."

6 Die Beklagten versandten mehr als 100.000 derartige Schreiben an verschiedene Webseiten-Betreiber.

7 Der Kläger überwies am 25. Oktober 2022 den Betrag von 170 € auf das im Schreiben angegebene Konto des Beklagten zu 2. Aufgrund von Medienberichten über das Vorgehen der Beklagten forderte der Kläger diesen Betrag - erfolglos - vom Beklagten zu 1 zurück.

8 Das Amtsgericht hat den Beklagten zu 1 verurteilt, an den Kläger 70 € nebst Zinsen zu zahlen, und die Klage im Übrigen abgewiesen. Auf die Berufung des Klägers hat das Landgericht das erstinstanzliche Urteil abgeändert und die Beklagten als Gesamtschuldner verurteilt, an den Kläger 170 € nebst Zinsen zu zahlen.

9 Das Berufungsgericht hat zur Begründung seiner Entscheidung unter anderem ausgeführt, dem Kläger stehe gegen die Beklagten als Gesamtschuldner der geltend gemachte Anspruch aus § 826 BGB zu. Die Beklagten hätten dem Kläger vorsätzlich in einer gegen die guten Sitten verstoßenden Weise einen Schaden zugefügt. Dem Beklagten zu 1 habe wegen des streitgegenständlichen Sachverhalts gegen den Kläger der in dem "Abmahnschreiben" als bestehend beschriebene Anspruch nicht gemäß Art. 82 Abs. 1 DSGVO zugestanden. Ein Verstoß gegen die Datenschutz-Grundverordnung liege bereits deshalb nicht vor, weil mit der Weitergabe der dynamischen IP-Adresse des Beklagten zu 1 an Google USA kein personenbezogenes Datum im Sinne der Verordnung betroffen

sei. Auch sei dem Beklagten zu 1 kein Schaden im Sinne des Art. 82 Abs. 1 DSGVO entstanden. Ein Schadensersatzanspruch des Beklagten zu 1 sei zudem jedenfalls wegen Rechtsmissbrauchs ausgeschlossen. Wer - wie der Beklagte zu 1 - einen Verstoß gegen sein Persönlichkeitsrecht gezielt provoziere, um daraus hiernach Ansprüche zu begründen, verstoße gegen das Verbot selbstwidersprüchlichen Verhaltens und sei nicht schutzbedürftig. Zu dem Umstand, dass dem Beklagten zu 1 die in dem "Abmahn schreiben" als bestehend dargestellten Ansprüche nicht zustünden, kämen vorliegend weitere besondere, die Sittenwidrigkeit begründende Umstände hinzu.

10 Mit ihrer vom Berufungsgericht zugelassenen Revision erstreben die Beklagten die Wiederherstellung des erstinstanzlichen Urteils.

11 B. Möglicherweise auf den Fall anwendbare Vorschriften des nationalen Rechts

12 Bürgerliches Gesetzbuch (BGB)

13 § 812 Herausgabeanspruch

14 (1) Wer durch die Leistung eines anderen oder in sonstiger Weise auf dessen Kosten etwas ohne rechtlichen Grund erlangt, ist ihm zur Herausgabe verpflichtet.

...

15 § 826 Sittenwidrige vorsätzliche Schädigung

16 Wer in einer gegen die guten Sitten verstoßenden Weise einem anderen vorsätzlich Schaden zufügt, ist dem anderen zum Ersatz des Schadens verpflichtet.

17 C. Zur Vorlage an den Gerichtshof

18 Der Erfolg der Revision hängt von der Auslegung des Unionsrechts ab. Der dem Kläger vom Berufungsgericht zugesprochene Anspruch auf Rückerstattung des von ihm auf das "Abmahnschreiben" hin gezahlten Betrages wegen sittenwidriger vorsätzlicher Schädigung durch die Beklagten (§ 826 BGB) kommt - ebenso wie ein Erstattungsanspruch des Klägers wegen ungerechtfertigter Bereicherung des Beklagten zu 1 nach § 812 Abs. 1 Satz 1 Alt. 1 BGB - nach nationalem Recht nur in Betracht, wenn dem Beklagten zu 1 aufgrund der Übermittlung seiner dynamischen IP-Adresse an Google USA aufgrund des Besuchs der vom Kläger betriebenen Website kein Anspruch auf Ersatz immateriellen Schadens nach Art. 82 Abs. 1 DSGVO gegen den Kläger zustand. Insoweit wirft der Streitfall noch ungeklärte Fragen zur Auslegung des Unionsrechts auf. Vor einer Entscheidung ist deshalb das Verfahren auszusetzen und gemäß Art. 267 Abs. 1 Buchst. b und Abs. 3 AEUV eine Vorabentscheidung des Gerichtshofs der Europäischen Union (im Folgenden: Gerichtshof) einzuholen.

19 I. Zur ersten Vorlagenfrage:

20 1. Das Berufungsgericht hat angenommen, ein Anspruch des Beklagten zu 1 gegen den Kläger nach Art. 82 Abs.1 DSGVO habe bereits deshalb nicht bestanden, weil mit der Weitergabe der dynamischen IP-Adresse des Beklagten zu 1 an Google USA kein personenbezogenes Datum im Sinne der Verordnung betroffen sei. Zwar könne eine dynamische IP-Adresse ein personenbezogenes Datum in diesem Sinne sein, wenn die Identität der betroffenen Person anhand der IP-Adresse bestimmbar sei. Dies sei im Hinblick auf den Beklagten zu 1 aber nicht der Fall gewesen, weil weder dargetan noch sonst ersichtlich sei, dass Google USA über rechtliche Mittel verfüge, die vernünftigerweise eingesetzt wer-

den könnten, um ihn mit Hilfe Dritter anhand der IP-Adresse bestimmen zu lassen. Es hat seiner Prüfung der Bestimmbarkeit des Betroffenen also einen relativen Maßstab zugrunde gelegt (vgl. zum Unterschied zwischen objektivem und relativem Maßstab in diesem Zusammenhang Senatsbeschluss vom 28. Oktober 2014 - VI ZR 135/13, ECLI:DE:BGH:2014:281014BVIZR135.13.0, VersR 2015, 370 Rn. 23 ff.) und insoweit auf den Empfänger der übermittelten IP-Adresse abgestellt.

21 Das Berufungsgericht hat seine Auffassung im rechtlichen Ausgangspunkt dabei auf das - auf eine Vorlage des Senats zur Vorabentscheidung (vgl. Senatsbeschluss vom 28. Oktober 2014 - VI ZR 135/13, ECLI:DE:BGH:2014:281014BVIZR135.13.0, VersR 2015, 370) hin ergangene - Urteil des Gerichtshofs vom 19. Oktober 2016 im Verfahren C-582/14 gestützt, wonach Art. 2 Buchst. a der Richtlinie 95/46 EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutzrichtlinie; ABl. L 281 vom 23. November 1995, S. 31) dahin auszulegen ist, dass eine dynamische IP-Adresse, die von einem Anbieter von Online-Medien diensten beim Zugriff einer Person auf eine Website, die dieser Anbieter allgemein zugänglich macht, gespeichert wird, für den Anbieter ein personenbezogenes Datum im Sinne der genannten Bestimmung darstellt, wenn er über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen (ECLI:EU:C:2016:779, CR 2016, 791 Rn. 49).

22 2. Der Senat hat Zweifel, ob sich aus dieser Entscheidung des Gerichtshofs, wie vom Berufungsgericht angenommen, ableiten lässt, im Streitfall sei der sachliche Anwendungsbereich der Datenschutz-Grundverordnung nach Art. 2 Abs. 1, Art. 4 Nr. 1 DSGVO nur eröffnet, wenn Google USA über rechtliche Mittel

verfügte, die vernünftigerweise eingesetzt werden konnten, um den Beklagten zu 1 mit Hilfe Dritter anhand der auf Veranlassung des Klägers übermittelten IP-Adresse bestimmen zu lassen:

23

Gemäß Art. 4 Nr. 1 DSGVO bezeichnet der Ausdruck "personenbezogene Daten" im Sinne der Verordnung alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person ("betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. Der Senat teilt zwar die Auffassung des Berufungsgerichts, dass hinsichtlich der Fragen, wann sich gemäß Art. 4 Nr. 1 DSGVO Informationen auf eine "identifizierte" oder "identifizierbare" Person beziehen und ob insoweit ein objektiver oder relativer Maßstab anzulegen ist, grundsätzlich auf die Rechtsprechung des Gerichtshofs dazu zurückgegriffen werden kann, wann Informationen eine "bestimmte" oder "bestimmbare" Person im Sinne von Art. 2 Buchstabe a der Datenschutzrichtlinie betreffen. Denn der Inhalt der jeweiligen Definition des Begriffs "personenbezogene Daten" ist in beiden Vorschriften im Wesentlichen identisch (vgl. Karg in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2. Aufl., Art. 4 Nr. 1 DSGVO Rn. 6; Klar/Kühling in Kühling/Buchner, DSGVO BDSG, 4. Aufl., Art. 4 Nr. 1 DSGVO Rn. 2; Klabunde/Horváth in Ehmann/Selmayr, Datenschutz-Grundverordnung, 3. Aufl., Art. 4 Rn. 8; Ziebarth in Sydow/Marsch, DSGVO/BDSG, 3. Aufl., Art. 4 DSGVO Rn. 7). Fraglich erscheint aber, ob sich aus der Rechtsprechung des Gerichtshofs ergibt, dass die Personenbezogenheit einer an einen Dritten übermittelten Information nur dann bejaht werden kann, wenn der Empfänger anhand der Information eine natürliche Person identifizieren kann.

24 Zum einen ist nicht ersichtlich, warum der sachliche Anwendungsbereich der Datenschutz-Grundverordnung nicht (auch) dann eröffnet sein soll, wenn der als Verantwortliche in Anspruch genommenen übermittelnden Stelle die Identifizierung einer natürlichen Person anhand der übermittelten Information möglich ist, sie also - gegebenenfalls mit Hilfe eines Dritten - den Personenbezug herstellen kann. Denn grundsätzlich sind - bei Heranziehung eines relativen Maßstabs für die Prüfung der Personenbezogenheit einer Information - die Verhältnisse der verantwortlichen Stelle zu berücksichtigen (vgl. Senatsbeschluss vom 28. Oktober 2014 - VI ZR 135/13, ECLI:DE:BGH:2014:281014BVIZR135.13.0, VersR 2015, 370 Rn. 25). Dementsprechend hat der Gerichtshof in seinem Urteil vom 19. Oktober 2016 im Verfahren C-582/14 auf die Verhältnisse des als für die Speicherung der IP-Adresse verantwortliche Stelle in Anspruch genommenen Anbieters des Online-Mediendienstes abgestellt (vgl. EuGH, ECLI:EU:C:2016:779, CR 2016, 791 Rn. 47 ff.).

25 Zum anderen stand in dem dem Urteil des Gerichtshofs vom 19. Oktober 2016 im Verfahren C-582/14 zugrundeliegenden Sachverhalt die Zulässigkeit der Speicherung einer dynamischen IP-Adresse in Rede. Geht es um die Speicherung einer Information, leuchtet es ein, deren Personenbezogenheit danach zu beurteilen, ob die speichernde Stelle anhand der Information eine natürliche Person identifizieren kann. Denn andernfalls kann mit der Speicherung - auch aus Sicht des Betroffenen - kein Risiko der Identifizierung einhergehen. Im Streitfall hat der Beklagte zu 1 jedoch nicht die Speicherung seiner IP-Adresse durch den Kläger oder durch Google USA, sondern deren Übermittlung an Google USA im Rahmen des Besuchs der Website des Klägers beanstandet. Mit der Übermittlung der Information hat die übermittelnde Stelle jedoch nicht allein das Risiko einer Identifizierung durch diesen Empfänger geschaffen, sondern darüber hinaus die Möglichkeit einer weiteren Verbreitung der Information und damit letztlich einer Identifizierung durch beliebige Dritte eröffnet. Dies könnte dafür sprechen,

die Personenbezogenheit der Information - soweit es um die Rechtmäßigkeit ihrer Übermittlung geht - anhand eines objektiven Maßstabes danach zu beurteilen, ob sie generell geeignet ist, eine natürliche Person zu identifizieren, es also genügt, wenn - irgendwelche - Dritte in der Lage sind, die Identität des Betroffenen anhand der übermittelten Information festzustellen. Dies wäre hinsichtlich der dynamischen IP-Adresse der Fall, weil jedenfalls der Internetzugangsanbieter in der Lage ist, anhand der IP-Adresse den Nutzer der Website zu bestimmen. Dementsprechend hat das Gericht der Europäischen Union in einem vergleichbaren Fall die Übermittlung einer dynamischen IP-Adresse als die Übermittlung eines personenbezogenen Datums angesehen und dabei allein darauf abgestellt, dass selbst sogenannte "dynamische" IP-Adressen, die wesensbedingt ständig wechselten, zum Zeitpunkt des Besuchs der Website einer bestimmten Person zugewiesen seien (vgl. EuG, ECLI:EU:T:2025:4, r + s 2025, 228 Rn. 122). Durch den Gerichtshof ist die Frage aber noch nicht eindeutig geklärt.

26

3. Sollte es für die Beurteilung der Personenbezogenheit einer übermittelten Information darauf ankommen, ob gerade der für die Übermittlung Verantwortliche oder der Empfänger (rechtlich und tatsächlich) über Mittel verfügen, die vernünftigerweise eingesetzt werden können, um die betreffende Person - gegebenenfalls mit Hilfe eines Dritten - bestimmen zu lassen, stellt sich die Frage, ob es genügt, dass für diese Stellen unter bestimmten Voraussetzungen Möglichkeiten zur Identifizierung der betroffenen Person bestehen können, für sie also die abstrakte Möglichkeit einer Identifizierung besteht, oder ob diese Voraussetzungen in tatsächlicher und rechtlicher Sicht im konkreten Fall auch vorgelegen haben müssen. Diese Frage erscheint durch die bisherige Rechtsprechung des Gerichtshofs noch nicht eindeutig geklärt (vgl. Klar/Kühling in Kühling/Buchner, DSGVO BDSG, 4. Aufl., Art. 4 Nr. 1 DSGVO Rn. 28; Arning/Rothkegel in Taeger/Gabel, DSGVO - BDSG - TTDSG, 4. Aufl., Art. 4 DSGVO Rn. 37).

- 27 Im Streitfall würden eine abstrakte und eine konkrete Betrachtungsweise zu jeweils unterschiedlichen Ergebnissen führen. So besteht zwar prinzipiell sowohl für den Kläger als auch für Google USA nach nationalem Recht die rechtliche Möglichkeit, im Falle einer von der Bundesrepublik Deutschland aus verursachten Schädigung Strafanzeige bei den Strafverfolgungsbehörden zu erstatten oder sich im Falle einer drohenden Schädigung an die zur Gefahrenabwehr zuständigen Behörden zu wenden. Die für die Verfolgung von Straftaten und Ordnungswidrigkeiten zuständigen Behörden können nach § 100j Abs. 1 und 2 StPO, § 174 Abs. 1 Satz 3 iVm Abs. 5 Nr. 1 TKG unter bestimmten Voraussetzungen von Internetzugangsanbietern Auskunft über anhand einer IP-Adresse einer natürlichen Person zugeordnete Bestandsdaten verlangen und so den Betreffenden identifizieren. Eine derartige Auskunftsmöglichkeit besteht auch - bei bestimmten, qualifizierten Gefahrenlagen - für die für die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung zuständigen Behörden (§ 174 Abs. 1 Satz 3 iVm Abs. 5 Nr. 2 TKG). Weiterhin kann eine entsprechende Auskunft gemäß § 101 Abs. 2 Satz 1 Nr. 3 UrhG der von einer offensichtlichen Urheberrechtsverletzung Betroffene verlangen (vgl. BGH, Beschluss vom 5. Dezember 2012 - I ZB 48/12, ECLI:DE:BGH:2012:051212BIZB48.12.0, GRUR 2013, 536 Rn. 32 ff.).
- 28 Tatsächliche Voraussetzung für eine Identifizierung des Anschlussinhabers anhand der IP-Adresse auf diesen Wegen ist aber zunächst, dass die in Rede stehende IP-Adresse von der Auskunft suchenden Stelle dem Internetzugangsanbieter mitgeteilt werden kann. Im Streitfall ist aber nicht festgestellt, dass die dem Beklagten zu 1 beim Besuch der Website des Klägers zugewiesene dynamische IP-Adresse vom Kläger oder von Google USA für eine Zeitdauer gespeichert wurde, die eine entsprechende Anfrage beim Internetzugangsanbieter ermöglicht hätte. Das Berufungsgericht hat zudem nicht festgestellt, dass die dargestellten rechtlichen Voraussetzungen für ein Auskunftersuchen im Streitfall erfüllt sind.

29 II. Zur zweiten Vorlagefrage:

30 1. Das Berufungsgericht hat offen gelassen, ob die Übermittlung der IP-Adresse an Google USA im Einklang mit den Vorschriften der Datenschutz-Grundverordnung - bei Unterstellung der Eröffnung ihres sachlichen Anwendungsbereichs - stand. Im Revisionsverfahren ist daher davon auszugehen, dass die Voraussetzungen für eine Übermittlung von personenbezogenen Daten an ein Drittland (Art. 6 f., Art. 44 ff. DSGVO) nicht erfüllt waren und ein Verstoß gegen die Verordnung im Sinne des Art. 82 Abs. 1 DSGVO vorlag. Das Berufungsgericht ist jedoch der Ansicht, dem Beklagten zu 1 sei kein Schaden im Sinne des Art. 82 Abs. 1 DSGVO entstanden. Dass die Weitergabe der IP-Adresse bei dem Kläger einen immateriellen Schaden in dem Sinne verursacht hätte, dass er die Befürchtung gehegt habe, seine IP-Adresse werde in Zukunft missbräuchlich verwendet, könne unter den gegebenen besonderen Umständen und im Hinblick auf den Beklagten zu 1 als betroffene Person nicht festgestellt werden.

31 Der Begriff "Schaden" - so das Berufungsgericht - könne naturgemäß nur so verstanden werden, dass es sich um eine unfreiwillige Einbuße - hier bezüglich der Kontrolle über die eigenen Daten - handeln müsse. Der Beklagte zu 1 habe sich der Kontrolle über seine jeweilige IP-Adresse aber gerade nicht unfreiwillig begeben. Er habe die klägerische Website nicht aufgesucht, um sich dort über die Angebote des Klägers zu informieren, sondern nur im Zusammenhang mit der Erhebung des Vorwurfs des Datenschutzverstoßes gegen diesen. Dies habe er in dem sicheren Wissen getan, dass bei einem entsprechenden Treffer (Verwendung der dynamischen Variante von Google Fonts auf der mittels des Webcrawlers aufgefundenen Website) und Aufruf der Seite die dann an ihn vergebene dynamische IP-Adresse an Google USA weitergeleitet werden würde. Zudem spreche die Vielzahl der vom Beklagten zu 1 indizierten Vorgänge dieser Art - unstreitig jedenfalls mehr als 100.000 Fälle - schon per se dagegen, dass

der Beklagte zu 1 tatsächlich die Befürchtung einer missbräuchlichen Verwendung seiner IP-Adresse gehabt habe. Zu berücksichtigen sei in diesem Zusammenhang auch, dass der Beklagte zu 1 die Website des Klägers gerade nicht selbst aufgesucht habe, sondern der Webseiten-Aufruf ausschließlich technisch mittels entsprechender Software initiiert worden sei. Zwar sei nicht per se auszuschließen, dass auch infolge technisch vermittelter bzw. dokumentierter Datenschutzverstöße ein Schaden im Sinne des Art. 82 DSGVO entstehen könne. Dazu bedürfe es dann aber entsprechender Umstände, die die besondere Betroffenheit der hinter der eingesetzten Software stehenden Personen begründeten. Derartige Umstände seien hier beklagtenseits weder dargetan noch sonst ersichtlich.

32

2. Diesen Ausführungen des Berufungsgerichts liegt ein im nationalen Recht verbreiteter sogenannter "natürlicher" Schadensbegriff zugrunde, wonach unter Schaden "jede unfreiwillige Einbuße an materiellen und immateriellen Gütern in Folge eines bestimmten Ereignisses" zu verstehen ist, freiwillige Einbußen also - zumindest in der Regel - keinen Schaden darstellen (vgl. etwa BeckOGK/Brand, Stand 1.3.2024, BGB § 249 Rn. 8 ff. mwN). 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 jedoch autonom unionsrechtlich zu definieren (st. Rspr., EuGH, ECLI:EU:C:2024:536, DB 2024, 1676 Rn. 31; ECLI:EU:C:2024:72, CR 2024, 160 Rn. 64; ECLI:EU:C:2023:370, VersR 2023, 920 Rn. 30 und 44). 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, ECLI:EU:C:2024:536, DB 2024, 1676 Rn. 25; ECLI:EU:C:2024:288, NJW 2024, 1561 Rn. 34; ECLI:EU:C:2023:370, VersR 2023, 920 Rn. 42).

33 Aus der im ersten Satz des 85. Erwägungsgrundes der Datenschutz-Grundverordnung enthaltenen beispielhaften Aufzählung der "Schäden", die den betroffenen Personen entstehen können, geht hervor, dass der Unionsgesetzgeber unter den Begriff "Schaden" insbesondere auch den bloßen "Verlust der Kontrolle" 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 (vgl. EuGH, ECLI:EU:C:2024:827, DB 2024, 2952 Rn. 145 mwN).

34 Nicht nur aus dem Wortlaut von Art. 82 Abs. 1 DSGVO im Licht ihrer Erwägungsgründe 85 und 146, wonach der Begriff "immaterieller Schaden" im Sinne dieses Artikels weit zu verstehen ist, sondern auch aus dem mit der Datenschutz-Grundverordnung verfolgten Ziel der Gewährleistung eines hohen Schutzniveaus für natürliche Personen bei der Verarbeitung personenbezogener Daten ergibt sich, dass die durch einen Verstoß gegen die Datenschutz-Grundverordnung ausgelöste Befürchtung einer betroffenen Person, ihre personenbezogenen Daten könnten von Dritten missbräuchlich verwendet werden, für sich genommen einen "immateriellen Schaden" im Sinne von Art. 82 Abs. 1 DSGVO darstellen kann (vgl. EuGH, ECLI:EU:C:2024:827, DB 2024, 2952 Rn. 144 mwN).

35 Wenn sich eine Person, die auf der Grundlage von Art. 82 Abs. 1 DSGVO Schadensersatz fordert, auf die Befürchtung beruft, dass ihre personenbezogenen Daten in Zukunft aufgrund eines solchen Verstoßes missbräuchlich verwen-

det werden, ist zu prüfen, ob diese Befürchtung unter den gegebenen besonderen Umständen und im Hinblick auf die betroffene Person als begründet angesehen werden kann (vgl. EuGH, ECLI:EU:C:2024:827, DB 2024, 2952 Rn. 143 mwN). Die bloße Behauptung einer Befürchtung ohne nachgewiesene negative Folgen reicht nicht aus (vgl. EuGH, ECLI:EU:C:2024:536, DB 2024, 1676. Rn. 35). Ein rein hypothetisches Risiko der missbräuchlichen Verwendung durch einen unbefugten Dritten kann nicht zu einer Entschädigung führen (vgl. EuGH, ECLI:EU:C:2024:72, DB 2024, 519 Rn. 68).

36 3. Ausgehend von diesen Grundsätzen könnte man im Streitfall einen immateriellen Schaden des Beklagten zu 1 in einem Kontrollverlust über seine personenbezogenen Daten durch die Übermittlung seiner IP-Adresse an Google USA sehen. Grundsätzlich könnte eine unbefugte Übermittlung personenbezogener Daten an einen Dritten geeignet sein, bei der betroffenen Person die berechtigte Befürchtung einer missbräuchlichen Verwendung dieser Daten zu begründen. Dass vorliegend mit der Übermittlung lediglich ein rein hypothetisches Risiko der missbräuchlichen Verwendung der IP-Adresse durch einen unbefugten Dritten verbunden gewesen wäre, hat das Berufungsgericht nicht festgestellt.

37 Auf der anderen Seite könnte der Annahme einer entsprechenden Befürchtung entgegenstehen, dass es der Beklagte zu 1 gezielt auf die Übermittlung der Daten angelegt hat. Ob die vom Berufungsgericht als maßgeblich angesehenen Umstände, nämlich die Tatsache, dass der Beklagte zu 1 die Übermittlung seiner IP-Adresse an Google USA - in einer Vielzahl von Fällen und in automatisierter Weise - bewusst und allein zu dem Zweck herbeigeführt hat, den Verstoß dokumentieren und gegenüber dem Verantwortlichen geltend machen zu können, der Annahme eines immateriellen Schadens im Sinne des Art. 82 Abs. 1 DSGVO entgegenstehen, ist durch die genannte Rechtsprechung des Gerichtshofs noch nicht geklärt.

38 III. Zur dritten Vorlagefrage:

39 Wenn in einem Fall wie dem vorliegenden ein immaterieller Schaden im Sinne des Art. 82 Abs. 1 DSGVO bejaht werden kann, stellt sich die Frage, ob dem Beklagten zu 1 dennoch aufgrund des Verbots des Rechtsmissbrauchs kein Schadensersatzanspruch nach Art. 82 Abs. 1 DSGVO zugestanden hat, wie das Berufungsgericht hilfsweise angenommen hat.

40 1. Nach ständiger Rechtsprechung des Gerichtshofs ist die missbräuchliche Berufung auf Unionsrecht nicht gestattet (vgl. etwa EuGH, ECLI:EU:C:2025:3, juris Rn. 49; ECLI:EU:C:2023:1014, WM 2024, 249 Rn. 281; ECLI:EU:C:2019:134, juris Rn. 96; ECLI:EU:C:2016:604, juris Rn. 37; jeweils mwN). Das gilt auch im Verhältnis unter Privaten (vgl. EuGH, ECLI:EU:C:2016:604, juris Rn. 2, 37). Der Nachweis einer missbräuchlichen Praxis setzt zum einen eine Gesamtheit objektiver Umstände voraus, aus denen sich ergibt, dass trotz formaler Einhaltung der in der Unionsregelung vorgesehenen Bedingungen das Ziel dieser Regelung nicht erreicht wurde, und zum anderen ein subjektives Element, nämlich die Absicht, sich einen aus der Unionsregelung resultierenden Vorteil zu verschaffen, indem die Voraussetzungen für seine Erlangung künstlich geschaffen werden (vgl. EuGH, ECLI:EU:C:2023:1014, WM 2024, 249 Rn. 285; ECLI:EU:C:2019:135, juris Rn. 97; ECLI:EU:C:2005:491, juris Rn. 39; jeweils mwN).

41 Die Prüfung des Vorliegens einer missbräuchlichen Praxis verlangt, dass das nationale Gericht alle Tatsachen und Umstände des Einzelfalls berücksichtigt, einschließlich derjenigen aus der Zeit nach dem Vorgang, dessen missbräuchlicher Charakter geltend gemacht wird (EuGH, ECLI:EU:C:2023:1014, WM 2024, 249 Rn. 286 mwN). Es ist daher Sache der nationalen Gerichte, gemäß den Beweisregeln des nationalen Rechts - soweit dadurch die Wirksamkeit

des Unionsrechts nicht beeinträchtigt wird - zu prüfen, ob die genannten Tatbestandsmerkmale einer missbräuchlichen Praxis im Einzelfall vorliegen. Der Gerichtshof kann jedoch im Rahmen eines Vorabentscheidungsverfahrens gegebenenfalls Klarstellungen vornehmen, um dem vorlegenden Gericht eine Richtschnur für seine Auslegung zu geben (vgl. EuGH, ECLI:EU:C:2023:1014, WM 2024, 249 Rn. 287 mwN).

42 2. Entsprechend diesen Grundsätzen wird der Gerichtshof um Klarstellung gebeten, ob in einem Fall wie dem vorliegenden, in dem davon auszugehen ist, dass der Verstoß des Verantwortlichen gegen die Datenschutz-Grundverordnung bewusst und allein zu dem Zweck herbeiführt worden ist, den Verstoß dokumentieren und gegenüber dem Verantwortlichen geltend machen zu können, ein Schadensersatzanspruch nach Art. 82 Abs. 1 DSGVO wegen Rechtsmissbrauchs verneint werden kann (vgl. dazu auch Frage 7 des Vorabentscheidungsersuchens des Amtsgerichts Arnsberg vom 31. Juli 2024, Rechtssache C-526/24, ECLI:DE:AGAR:2024:0731.42C434.23.0).

43 a) Insoweit stellt sich zum einen die durch Auslegung des Unionsrechts zu beantwortende Frage, auf welche Ziele welcher Vorschriften der Datenschutz-Grundverordnung für die Beurteilung, ob eine rechtsmissbräuchliche Geltendmachung des Schadensersatzanspruches nach Art. 82 Abs. 1 DSGVO vorliegt, abzustellen ist.

44 b) Zum anderen besteht das Bedürfnis einer Klarstellung durch den Gerichtshof hinsichtlich der Feststellung des subjektiven Elements missbräuchlichen Verhaltens:

45 Der Gerichtshof hat in seinem Urteil vom 28. Juli 2016 im Verfahren C-423/15 zur Feststellung des subjektiven Tatbestandsmerkmals ausgeführt, es

müsse aus einer Reihe objektiver Anhaltspunkte ersichtlich sein, dass wesentlicher Zweck der fraglichen Handlungen die Erlangung eines ungerechtfertigten Vorteils ist. Zum Beweis für das Vorliegen dieses zweiten Tatbestandsmerkmals, das auf die Absicht der Handelnden abstellt, könne unter anderem der rein künstliche Charakter der fraglichen Handlungen berücksichtigt werden (ECLI:EU:C:2016:604, ZIP 2016, 1498 Rn. 40 f.). Aus Sicht des Senats würden danach die vom Berufungsgericht festgestellten Umstände zur Bejahung des Vorliegens des subjektiven Tatbestandsmerkmals des missbräuchlichen Verhaltens genügen. Denn nach den Feststellungen des Berufungsgerichts standen als Motivation für das Handeln des Beklagten zu 1 finanzielle Interessen zumindest deutlich im Vordergrund. Das Berufungsgericht konnte nicht feststellen, dass der Beklagte zu 1 mit der Vorbereitung und Versendung seiner "Abmahnschreiben" neben den finanziellen auch weitere Ziele verfolgte.

46 Der Gerichtshof hat in seinem oben genannten Urteil aber auch ausgeführt, das Missbrauchsverbot greife nicht, wenn die fraglichen Handlungen eine andere Erklärung haben können als nur die Erlangung eines Vorteils (EuGH, ECLI:EU:C:2016:604, ZIP 2016, 1498 Rn. 40 mwN). Dies könnte dahin verstanden werden, dass das nationale Gericht andere als finanzielle Motive ausschließen können muss, um den Missbrauchstatbestand zu bejahen. Dazu war das Berufungsgericht im vorliegenden Fall nicht in der Lage. Es konnte nicht ausschließen, dass es dem Beklagten zu 1 bei seinem Handeln auch darum gegangen ist, die Betreiber der Websites auf die mit der dynamischen Einbindung von

Google Fonts verbundene Datenschutzproblematik hinzuweisen.

von Pentz

Oehler

Allgayer

Böhm

Linder

Vorinstanzen:

AG Hannover, Entscheidung vom 12.07.2023 - 525 C 8451/22 -

LG Hannover, Entscheidung vom 01.07.2024 - 18 S 10/23 -

Verkündet am:

28. August 2025

Böhringer-Mangold, Justizamtsinspektorin
als Urkundsbeamtin der Geschäftsstelle