LG Augsburg, Endurteil v. 02.05.2023 – 031 O 1709/22

Titel:

Keine Ansprüche eines Nutzers gegen Betreiber von Facebook wegen Scraping-Vorfall

Normenketten:

DS-GVO Art. 5 Abs. 1 lit. a u. lit. f, Art. 6 Abs. 1, Art. 13, Art. 14, Art. 17, Art. 25 Abs. 2, Art. 82 Abs. 1
BGB § 823 Abs. 2, § 1004 Abs. 1 S. 2
GG Art. 1 Abs. 1, Art. 2 Abs. 1

Leitsätze:

1. Eine Social Media Plattform, deren Ziel es ist, Kontakte zu suchen und zu finden, ist nicht gem. Art. 25 Abs. 2 DS-GVO dazu verpflichtet, die Voreinstellungen so zu treffen, dass die Suchbarkeitsfunktion für die Telefonnummern der Nutzer gesperrt ist. (Rn. 32) (redaktioneller Leitsatz)
2. Ein Scraping-Vorfall stellt keinen nach Art. 33 DS-GVO meldepflichtigen Verstoß dar. (Rn. 33) (redaktioneller Leitsatz)
3. Ein nach Art. 82 Abs. 1 DS-GVO ersatzfähiger immaterieller Schaden muss zumindest einen realen und sicheren emotionalen Schaden bilden und nicht nur ein Ärgernis oder eine sonstige Unannehmlichkeit. (Rn. 35) (redaktioneller Leitsatz)

Schlagworte:

Datenschutzverstoß, Scraping

Fundstellen:

GRUR-RS 2023, 13778
ZD 2023, 639
LSK 2023, 13778

Tenor

1. Die Klage wird abgewiesen.

2. Der Kläger hat die Kosten des Rechtsstreits zu tragen.

3. Das Urteil ist vorläufig vollstreckbar. Der Kläger kann die Vollstreckung der Beklagten durch Sicherheitsleistung in Höhe von 110 % des aufgrund des Urteils vollstreckbaren Betrags abwenden, wenn nicht die Beklagte vor der Vollstreckung Sicherheit in Höhe von 110 % des zu vollstreckenden Betrags leistet.

Beschluss

Der Streitwert wird auf 5.500,00 € festgesetzt.

Tatbestand

1
Der Kläger fordert von der Beklagten wegen Verstößen gegen die Datenschutzgrundverordnung Schadensersatz, Unterlassung und Auskunft.

2
Die Beklagte ist Anbieterin der F.-Plattform auf dem Gebiet der Europäischen Union. Der Kläger ist deutscher Nutzer dieser Plattform; er meldet sich mit seiner E-Mail-Adresse an. Sein Name, Geschlecht und Nutzer-ID waren auf dem Nutzerkonto öffentlich einsehbar (Anlage B 15), denn es handelt sich bei diesen Informationen um immer öffentliche Nutzerinformationen. Die Sichtbarkeit der sonstigen Daten des Klägers (Telefonnummer, E-Mail-Adresse, Wohnort, Geburtsdatum, Stadt, Beziehungsstatus) war von der Zielgruppenauswahl des Klägers abhängig. Die Daten „Land“, „Bundesland“, „Geburtsort“ und „weitere korrelierende Daten“ entsprechen keinen Profilfeldern auf der F.-Plattform.

3

Bei der erstmaligen Anmeldung trägt der Nutzer die ihn betreffenden personenbezogenen Daten, konkret Vor- und Zuname, Handynummer oder E-Mail-Adresse, Geschlecht und Geburtsdatum, in die Registrierungsmaske ein. Er wird auf die Nutzungsbedingungen und nach der Registrierung auf eine Fülle an Einstellungen und Untereinstellungen hingewiesen. Insoweit hat die Beklagte Voreinstellungen getroffen.

4
Die Angabe der Telefonnummer kann für eine Sicherheitsabfrage (Passwort-Rücksetzung) verwendet werden. Im Profil des Klägers war die diesbezüglich verwendete Telefonnummer nicht öffentlich freigegeben und daher nicht öffentlich einsehbar, allerdings konnte der Kläger über seine Telefonnummer gefunden werden. Diese Einstellung war vorgegeben, aber dahingehend abänderbar, dass der Nutzer nicht anhand seiner Telefonnummer gefunden werden kann.

5
Die Beklagte verwendet einen Kontaktimporter (Contakt-Import-Tool; CIT) an. Dieser dient dazu, die im Smartphone eines Nutzers gespeicherten Personenkontakte mit Nutzern auf F. zu synchronisieren; dies geschieht über die hinterlegte, nicht-öffentliche Handynummer. Ebenso funktioniert die von der Beklagten betriebene F.-Messenger-App. Jegliches automatisiertes Sammeln von Daten (Scraping) ohne Erlaubnis war durch die Nutzungsbedingungen der Beklagten verboten.

6
Im Jahr 2019 generierten Unbekannte Telefonnummern und synchronisierten diese über das Kontaktimporter bzw. die F.-Messenger-App mit Profilen von F.nutzern. Die dort öffentlich abgelegten Daten wurden in der Folge abgeschöpft (gescrapt) und mit den Handynummern zusammengeführt (Anlage B 11).

7
Am 03.04.2021 veröffentlichte der Business Insider einen Artikel, wonach Informationen einer Vielzahl von F.-Nutzern von Dritten im Internet zugänglich gemacht worden seien. Die Beklagte wandte sich mit einem am 06.04.2021 in F. zugänglichen Artikel an ihre Nutzer (Anlage B 10).

8
Mit anwaltlicher E-Mail vom 02.11.2021 forderte der Kläger die Beklagte zur Zahlung von Schadensersatz in Höhe von € 500,- sowie zur Unterlassung und Auskunft auf (Anlage K 1). Die Beklagte antwortete mit anwaltlichem Schreiben vom 31.10.2021 (Anlage B 16).

9
Die irische Datenschutzbehörde DPC verhängte gegen die Beklagten mit Bescheid vom 25.11.2022 wegen Verstoßes gegen Art. 25 I und II DSGVO eine Geldbuße in Höhe von 265 Mio Euro und gab der Beklagten auf, Abhilfe zu schaffen (Anlage K 3).

10
Der Kläger trägt vor, dass seine E-Mail-Adresse, Wohnort, Geburtsdatum, Stadt, Beziehungsstatus, Telefonnummer in den durch Scraping abgerufenen Daten enthalten gewesen seien.

11
Der Kläger trägt weiter vor, er sei von einem Datenschutzvorfall betroffen; die Beklagte habe seine Daten unbefugten Dritten zugänglich gemacht. Eine im Darknet für jedermann abrufbare Datenbank enthalte seine Telefonnummer, seine F.-ID, seinen Namen, sein Geschlecht, seinen Wohnort, das Land, seinen Beziehungsstatus und seinen Arbeitgeber. Diese Datensätze seien z. B. auf der Seite raidformus.com veröffentlicht worden und ermöglichten böswilligen Akteuren eine weite Bandbreite von kriminellen Machenschaften wie etwa Identitätsdiebstahl, die Übernahme von Accounts, gezielte Phishing-Nachrichten oder „Sim-Swap“-Angriffe, um Passwörter zu ändern, die durch telefonnummernbasierende Authentifizierung geschützt sind.

12
Der Kläger behauptet ferner, er habe aufgrund der Veröffentlichung der gescrapten Daten einen erheblichen Kontrollverlust erlitten und sei in einem Zustand des großen Unwohlseins und großer Sorge über möglichen Missbrauch seiner Daten verblieben. Er erhalte seit der Veröffentlichung unregelmäßig unbekannte Kontaktversuche via SMS und E-Mail. Diese enthielten Nachrichten mit offensichtlichen Betrugsversuchen und potenziellen Virenlinks.

13

Der Kläger behauptet schließlich, die Beklagte habe keinerlei Sicherheitsvorkehrungen gegen die Ausnutzung des Contakt-Import-Tools getroffen, insbesondere nicht sichergestellt, dass es sich bei der Anfrage der Synchronisierung um die Anfrage eines Menschen und nicht eines Computerprogramms gehandelt habe; ebenso wenig sei die Plausibilität der Anfragen überprüft worden, etwa indem ungewöhnlich viele Anfragen derselben IP-Adresse oder mit auffälligen Telefonnummernabfolgen automatisch abgelehnt worden wären.

14
Der Kläger behauptet endlich, die Beklagte habe den Kläger zu keinem Zeitpunkt darüber informiert, dass seine Daten durch Dritte entwendet und veröffentlicht wurden; sie habe auch die zuständige Datenschutzbehörde in Irland nicht über den Vorfall informiert.

15
Der Kläger ist der Ansicht, die Klage sei zulässig, insbesondere bestimmt genug und es bestehe ein Feststellungsinteresse. Der Schadensersatzanspruch ergebe sich aus Art. 82 DSGVO. Der Schutzbereich sei eröffnet, die Beklagte habe gegen mehrere Pflichten der DSGVO verstoßen (Verletzung der Transparenzpflichten, Verletzung der Pflicht zur Gewährleistung angemessener technischer und organisatorischer Maßnahmen, Verletzung der Pflicht zu datenschutzfreundlichen Voreinstellungen, Verletzung der Benachrichtigungs- und Meldepflicht sowie der Auskunftspflicht)

16
Der Kläger ist ferner der Meinung, die Beklagte habe mangels wirksamer Einwilligung des Klägers seine Daten ohne Rechtsgrundlage und ausreichende Information verarbeitet; die Beklagte treffe die Darlegungs- und Beweislast.

17
Der Kläger beantragt zu erkennen:

1. Die Beklagte wird verurteilt, an die Klägerseite immateriellen Schadensersatz in angemessener Höhe zu zahlen, dessen Höhe in das pflichtgemäße Ermessen des Gerichts gestellt wird, mindestens jedoch 1.000,00 € nebst Zinsen seit Rechtshängigkeit in Höhe von fünf Prozentpunkten über dem Basiszinssatz.

2. Es wird festgestellt, dass die Beklagte verpflichtet ist, der Klägerseite alle künftigen Schäden zu ersetzen, die der Klägerseite durch den unbefugte Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussage der Beklagten im Jahr 2019 erfolgte, entstanden sind und/oder noch entstehen werden.

3. Der Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu € 250.000,00, ersatzweise in ihrem gesetzlichen Vertreter (Director) zu vollstreckenden Ordnungshaft, oder an einer ihrem gesetzlichen Vertreter (Director) zu vollstreckenden Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen,

a) personenbezogene Daten der Klägerseite namentlich, Telefonnummer, F.-ID, Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus unbefugten Dritten über eine Software zum Importieren von Kontakten zugängig zu machen, ohne die nach dem Stand der Technik möglichen Sicherheitsmaßnahmen vorzusehen, um die Ausnutzung des Systems für andere Zwecke als der Kontaktaufnahme zu verhindern,

b) die Telefonnummer der Klägerseite auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt wurde, namentlich ohne eindeutige Informationen darüber, dass die Telefonnummer auch bei Einstellung auf „privat“ nach der Verwendung des Kontaktimporttools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert wird und im Falle der Nutzung der F.-Messenger-App, hier ebenfalls explizit die Berechtigung verweigert wird.

4. Die Beklagte wird verurteilt, der Klägerseite Auskunft über die Klägerseite betreffende personenbezogenen Daten, welche die Beklagte verarbeitet, zu erteilen, namentlich welche Daten durch welche Empfänger zu welchem Zeitpunkt bei der Beklagten durch Scraping oder durch Anwendung des Kontaktimporttools erlangt werden konnten.

5. Die Beklagte wird verurteilt, an die Klägerseite vorgerichtliche Rechtsanwaltskosten in Höhe von 887,03 € zu zahlen, zuzüglich Zinsen seit Rechtshängigkeit in Höhe von fünf Prozentpunkten über dem Basiszinssatz.

18
Die Beklagte beantragt,

Klageabweisung.

19
Die Beklagte ist der Ansicht, die Klage sei weitgehend schon unzulässig, da die Klageanträge 1) bis 3) zu unbestimmt seien und der Feststellungsklage das Feststellungsinteresse fehle. Die Voraussetzungen für einen Schadensersatzanspruch nach Art. 82 DSGVO lägen nicht vor. Scraping sei kein Hacking. Weder sei der Schutzbereich eröffnet, noch lägen Verstöße gegen die DSGVO vor. Zudem fehle es an einem kausalen immateriellen Schaden, insbesondere reiche der von der Klageseite behauptete Kontrollverlust nicht aus. Die Klägerin treffe die Darlegungs- und Beweislast. Ferner fehle es an einem Verschulden der Beklagten.

20
Wegen der weiteren Einzelheiten wird auf die gewechselten Schriftsätze sowie das Protokoll der mündlichen Verhandlung vom 28.03.2023 Bezug genommen.

Entscheidungsgründe

21
Die zulässige Klage ist unbegründet.

22
I. Die Klage ist zulässig.

23
1. Das Landgericht Augsburg ist international gemäß Art. 79 II DSGVO und Art. 18 I Alt. 2 iVm Art. 17 I lit. c) VO (EU) 1215/2012 zuständig. Der Kläger hat seinen gewöhnlichen Aufenthaltsort bzw. seinen Wohnsitz in und damit im hiesigen Gerichtsbezirk. Die Beklagte betreibt die Plattform gewerblich; der Kläger nutzt die Plattform für private Zwecke und ist damit Verbraucher.

24
2. Die Anträge sind hinreichend bestimmt genug iSd § 253 II Nr. 2 ZPO. Dies gilt sowohl für den Antrag Ziffer 1 als auch für den Antrag Ziffer 3a und 3b (dazu: LG Kiel GRUR-RS 2023, 328 Tz. 25 bis 29 sowie LG Aachen GRUR-RS 2023, 2621 Tz. 32 bis 36 und 38 bis 40 zu den jeweils identischen Klageanträgen wie im vorliegenden Fall). Auch das Feststellungsinteresse bezüglich des Antrags Ziffer 2 ist zu bejahen (LG Kiel GRUR-RS 2023, 328 Tz. 30 sowie LG Aachen GRUR-RS 2023, 2621 Tz. 37).

25
II. Die Klage hat in der Sache keinen Erfolg.

26
1. Dem Kläger steht gegen die Beklagte kein Anspruch auf Zahlung eines immateriellen Schadensersatzes zu.

27
a) Ein solcher Anspruch ergibt sich nicht aus Art. 82 I DSGVO.

28
aa) Es fehlt auf der Grundlage des klägerischen Vorbringens bereits an einem Verstoß gegen die Bestimmungen der Datenschutzgrundverordnung.

29
(1) Ein Verstoß gegen die Transparenzpflichten aus Artt. 5 I lit. a), 13, 14 DSGVO liegt nicht vor. Die von der Klagepartei vorgelegten Screenshots zu den Abläufen und Unterstrukturen des Internetauftritts der Beklagten sind hinreichend verständlich und transparent gestaltet. Der Kläger als Nutzer ist verpflichtet, sich sorgfältig mit den Hinweisen auseinanderzusetzen, um für sich eine Entscheidung zu treffen, in welchem Umfang er Informationen freigibt und wie weitgehend er die Kommunikationsplattform der Beklagten nutzen

will (ebenso: LG Aachen GRUR-RS 2023, 2621 Tz. 49 bis 55 sowie LG Kiel GRUR-RS 2023, 328 Tz. 37 bis 41).

30
(2) Es liegt auch kein Verstoß gegen die Datenschutzpflichten aus Artt. 5 I lit. f), 32 DSGVO vor.

31
Denn es wurde ausdrücklich darauf hingewiesen, dass Name, Profilbild, Titelbild, Geschlecht, Nutzername und Nutzer-ID für alle sichtbar sind; für einen Schutz dieser Daten bestand daher kein Anlass, da diese ohnehin öffentlich waren. Hinsichtlich der Telefonnummer des Klägers ist die Beklagte ihren Schutzpflichten ausreichend dadurch nachgekommen, dass sie in zureichender Weise darauf hingewiesen hat, dass der Kläger die Suchbarkeits-Einstellungen abändern kann (ebenso: LG Aachen GRUR-RS 2023, 2621 Tz. 56 bis 63 sowie LG Kiel GRUR-RS 2023, 328 Tz. 42f). Zudem war durch die Nutzungsbedingungen der Beklagten jegliches automatisiertes Sammeln von Daten (Scraping) ohne Erlaubnis der Beklagten verboten.

32
(3) Die Beklagte hat auch nicht gegen die Pflicht zu datenschutzfreundlichen Voreinstellungen gemäß Art. 25 I, II DSGVO verstoßen. Die Beklagte war insoweit insbesondere nicht verpflichtet, die Voreinstellung so zu treffen, dass eine durch den Kläger eingegebene Telefonnummer nicht dazu verwendet wird, ihn über eine Suchbarkeitsfunktion zu finden. Denn bei der von der Beklagten betriebenen Plattform handelt es sich um eine Sozial Media Plattform, deren Ziel es gerade ist, Kontakte zu suchen und zu finden. Eine Sperrung der Suchbarkeitsfunktion würde diesem Ziel diametral widersprechen (ebenso: LG Aachen GRUR-RS 2023, 2621 Tz. 64f sowie LG Kiel GRUR-RS 2023, 328 Tz. 44 bis 47). An dieser Einschätzung ändert sich auch nichts dadurch, dass die irische Datenschutzbehörde DPC gegen die Beklagten mit Bescheid vom 25.11.2022 wegen Verstoßes gegen Art. 25 I und II DSGVO eine Geldbuße in Höhe von 265 Mio Euro verhängt hat (Anlage K 3). Dabei kann dahinstehen, ob dieser Bescheid Bindungswirkung entfaltet, da er unstreitig noch nicht bestandskräftig ist (ebenso: LG Aachen GRUR-RS 2023, 2621 Tz. 66).

33
(4) Schließlich ist der Beklagten kein Verstoß gegen die Meldepflicht nach Art. 33 DSGVO vorzuwerfen, da es schon an einem meldepflichtigen Verstoß gegen die Datenschutzgrundverordnung fehlt (ebenso: LG Aachen GRUR-RS 2023, 2621 Tz. 67 sowie LG Kiel GRUR-RS 2023, 328 Tz. 48).

34
(5) Endlich liegt auch kein Verstoß gegen die Auskunftspflicht der Beklagten nach Art. 15 DSGVO vor. Denn die Beklagte hat gegenüber dem Kläger mit anwaltlichem Schreiben vom 31.10.2021 (Anlage B 16) Auskunft erteilt. Zu einer von Klageseite geforderte, darüber hinausgehende Auskunft war die Beklagte nicht verpflichtet; eine weitergehende Auskunft ist der Beklagten zudem nicht möglich. bb) Es fehlt ferner an einem immateriellen Schaden des Klägers.

35
(1) Zu den Anspruchsvoraussetzungen des Art. 82 I DSGVO zählt neben dem Verstoß gegen die Datenschutzgrundverordnung auch der Eintritt eines immateriellen Schadens (vgl. OLG Frankfurt GRUR 2022, 1252 Tz. 61 bis 64). In Anbetracht der Erwägungsgründe 75, 85, 146 und 148 der DSGVO hatte der Verordnungsgeber insoweit Diskriminierung, Identitätsdiebstahl, Identitätsbetrug, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden persönlichen Daten oder gesellschaftliche Nachteile ohne den Ausschluss von Bagatellschäden im Blick. Hinsichtlich eines möglichen künftigen Missbrauchs personenbezogener Daten wird ein immaterieller Schaden aber nur dann zu begründen sein, wenn es sich um einen realen und sicheren emotionalen Schaden handelt und nicht nur um ein Ärgernis oder eine Unannehmlichkeit (vgl. EuGH, Schlussanträge vom 27.04.2023 – C-340/21).

36
(2) Gemessen an diesen Maßstäben ist ein immaterieller Schaden des Klägers zu verneinen. Es blieb unklar, ob die Klageseite von einem Identitätsdiebstahl betroffen ist oder ihr Accout bei der Beklagten durch unbekannte Dritte übernommen wurde. Der Kläger ist – trotz Anordnung des persönlichen Erscheinens – im Termin zur mündlichen Verhandlung nicht erschienen und konnte daher dazu nicht angehört werden; dies geht zu seinen Lasten. Da allein durch das Bekanntwerden einer Telefonnummer ein Identitätsdiebstahl unwahrscheinlich ist (dazu: LG Karlsruhe, ZD 2022, 55) und die übrigen Daten des Klägers mit dessen Einwilligung ohnehin öffentlich sind, stellt die Möglichkeit eines künftigen Missbrauchs der klägerischen

Daten nur eine Unannehmlichkeit dar, die gerade keinen immateriellen Schaden zu begründen vermag. Schließlich darf nicht aus den Augen verloren werden, dass nicht die Beklagte, sondern unbekannte Dritte die Daten der Klagepartei gespcrapt und ins Darknet eingestellt haben sollen.

37
b) Ein Anspruch auf immateriellen Schadensersatz ergibt sich auch nicht aus nationalem Recht. Das ergibt sich schon daraus, dass nach § 253 I BGB wegen eines Schadens, der nicht Vermögensschaden ist, nur in den durch das Gesetz bestimmten Fällen gefordert werden kann. Die im Gesetz genannten Ausnahmen (§ 253 II BGB) liegen aber ebenso wenig vor, wie eine schwerwiegende Verletzung des Persönlichkeitsrechts des Klägers (Art. 1, 2 I GG).

38
2. Der Antrag des Klägers auf Feststellung, dass die Beklagte verpflichtet ist, alle künftige materiellen Schäden zu ersetzen, ist ebenfalls unbegründet. Denn es liegt kein Verstoß gegen die Bestimmungen der Datenschutzgrundverordnung vor (siehe oben Ziffer II 1 a aa).

39
3. Dem Kläger steht gegen die Beklagte ferner kein Anspruch auf Unterlassung der Verwendung der Kontakt-Importer-Software aus §§ 1004 I 2 BGB analog iVm Art. 1, 2 I GG oder aus § 823 II BGB iVm Artt. 6 I, 17 DSGVO zu. Auch insoweit fehlt es an einem Verstoß gegen die Bestimmungen der Datenschutzgrundverordnung (siehe oben Ziffer II 1 a aa).

40
4. Dem Kläger steht gegen die Beklagte auch kein Anspruch auf Unterlassung der Verarbeitung seiner Telefonnummer aus §§ 1004 I 2 BGB analog iVm Art. 1, 2 I GG oder aus § 823 II BGB iVm Artt. 6 I, 17 DSGVO zu. Auch insoweit fehlt es an einem Verstoß gegen die Bestimmungen der Datenschutzgrundverordnung (siehe oben Ziffer II 1 a aa).

41
5. Schließlich steht dem Kläger gegen die Beklagte kein Anspruch auf Auskunftserteilung nach Art. 15 I DSGVO zu. Dieser Anspruch ist gemäß § 362 I BGB erloschen, da die Beklagte mit anwaltlichem Schreiben vom 31.10.2021 (Anlage B 16) insoweit Auskunft erteilt hat. Soweit die Klageseite darüber hinaus Auskunft begehrt, inwieweit ihre Daten durch das Scraping von welchen Dritten verarbeitet wurden, ist ein Anspruch der Klageseite bereits dem Grund nach zu verneinen. Eine derartige Auskunft wäre der Beklagten zudem nicht möglich.

42
6. Mangels Hauptanspruch ist endlich ein Anspruch des Klägers auf Ersatz von vorgerichtlichen Rechtsanwaltskosten zu verneinen.

43
7. Andere, durchgreifende Anspruchsgrundlagen sind nicht ersichtlich.

44
III. 1. Die Kostenentscheidung ergibt sich aus § 91 I ZPO.

45
2. Die Entscheidung über die vorläufige Vollstreckbarkeit beruht auf §§ 708 Nr. 11, 711 S.1 und 2 ZPO.

46
3. Die Streitwertfestsetzung basiert auf § 63 II 1 GKG. Das Gericht bewertete die nicht bezifferten Anträge gemäß § 3 ZPO wie folgt: Ziffer 2: 1000,- €, Ziffer 3a: 1.500,- €, Ziffer 3b: 1.500,- € und Ziffer 4: 500,- €. Hinzu kam der bezifferte Zahlungsantrag Ziffer 1 mit € 1.000,-. Das ergibt insgesamt einen Streitwert von € 5.500,-. Die Anträge auf Zahlung von vorgerichtlichen Rechtsanwaltskosten und Zinsen hatten demgegenüber bei der Streitwertberechnung gemäß §§ 48 I 1 GKG iVm 4 I HS 2 ZPO außer Betracht zu bleiben.