OLG München, Verfügung v. 14.09.2023 – 14 U 3190/23 e

Titel:

Keine Unterlassungs- und Schadensersatzanspruch in "Scraping-Fällen"

Normenkette:

DSGVO Art. 82

Leitsätze:

1. Nicht jeder Kontrollverlust über persönliche Daten stellt einen Schaden im Sinne von Art. 82 DSGVO dar. (Rn. 96 – 102) (redaktioneller Leitsatz)

2. Der Betroffene eines "Sraping"-Vorfalls bei einem sozialen Netzwerk hat keinen Anspruch auf Unterlassung künftiger Verletzungen, wenn er diese durch Umstellung seiner Privatsphäre-Einstellung von "everyone" auf "friends of friends" verhindern kann. (Rn. 103 – 106) (redaktioneller Leitsatz)

Schlagworte:

Schadensersatz, Berufung, Erfolgsaussicht, Unterlassungsanspruch, Auskunft, Technik, Software, Pflichtverletzung, Daten, Schaden, Zustimmung, Einstellung, Verletzung, Anspruch, personenbezogene Daten, Stand der Technik, Verarbeitung personenbezogener Daten

Vorinstanz:

LG Kempten, Endurteil vom 23.06.2023 – 13 O 293/23

Rechtsmittelinstanzen:

OLG München, Berichtigungsbeschluss vom 12.10.2023 – 14 U 3190/23 e

OLG München, Beschluss vom 23.11.2023 – 14 U 3190/23

Fundstelle:

GRUR-RS 2023, 24733

Tenor

A. Der Senat beabsichtigt, die Berufung gegen das Urteil des Landgerichts Kempten (Allgäu) vom 05.02.2021, Az. 23 O 868/18, gemäß § 522 Abs. 2 ZPO zurückzuweisen, weil er einstimmig der Auffassung ist, dass die Berufung offensichtlich keine Aussicht auf Erfolg hat, der Rechtssache auch keine grundsätzliche Bedeutung zukommt, weder die Fortbildung des Rechts noch die Sicherung einer einheitlichen Rechtsprechung eine Entscheidung des Berufungsgerichts erfordert und die Durchführung einer mündlichen Verhandlung über die Berufung nicht geboten ist.

Entscheidungsgründe

1

B. Hintergrund ist folgende Einschätzung des Senats:

I.

2

Die Klagepartei beantragt in der Berufung:

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 EUR nebst Zinsen seit Rechtshängigkeit in Höhe von 5 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 unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussage der Beklagten im Jahr 2019 erfolgte, entstanden sind und/oder noch entstehen werden.

3. Die Beklagte wird verurteilt, es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu 250.000,00 EUR, ersatzweise an ihrem gesetzlichen Vertreter (Director) zu vollstreckender Ordnungshaft, oder einer an ihrem gesetzlichen Vertreter (Director) zu

vollstreckender Ordnungshaft bis zu sechs Monaten, im Wiederholungsfall bis zu zwei Jahren, zu unterlassen,

a. personenbezogene Daten der Klägerseite, namentlich Telefonnummer, Face-bookID, Familiennamen, Vornamen, Geschlecht, Bundesland, Land, Stadt, Beziehungsstatus unbefugten Dritten über eine Software zum Importieren von Kontakten zugänglich 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“ noch durch Verwendung des Kontaktimporttools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der Facebook-Messenger App, hier ebenfalls explizit die Berechtigung verweigert wird.

4. Die Beklagte wird verurteilt, der Klägerseite Auskunft über die Klägerseite betreffende personenbezogene 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 5 Prozentpunkten über dem Basiszinssatz.

3
Das entspricht dem erstinstanzlichen Begehren.

II.

4
Das Landgericht hat die Klage abgewiesen.

5
Auf Tatbestand und Gründe des angegriffenen Urteils nimmt der Senat Bezug.

6
1. Als unstreitig hat das Landgericht – von der Berufung insoweit nicht angegriffen – folgenden Sachverhalt dargestellt:

7
Die Beklagte betreibt die Plattform „Facebook“. Der Kläger nutzte einen Facebook-Account. Die Dienste der Beklagten ermöglichen es den Nutzern, persönliche Profile für sich zu erstellen und diese mit Freunden zu teilen. Die Nutzer können auf ihren persönlichen Profilen Angaben zu verschiedenen Daten zu ihrer Person einstellen. Dabei entscheiden sie – im von der Beklagten vorgegebenen Rahmen – darüber, welche anderen Gruppen von Nutzern auf ihre Daten zugreifen können.

8
Im Zeitraum Januar 2018 bis September 2019 wurden durch unbekannte Dritte Daten im Wege des so genannten „Scrapings“ abgeschöpft: Telefonnummern, Facebook-ID, Name, Vorname, Geschlecht und weitere Daten. Das „Scraping“ vollzog sich über das Tool „Contact-Import“. Indem eine Vielzahl von Kontakten in ein virtuelles Adressbuch eingegeben wurde, gelang es Unbekannten, die Telefonnummern konkreten Profilen zuzuordnen, ohne dass in den entsprechenden Profilen die hinterlegten Telefonnummern öffentlich freigegeben waren. Um die Telefonnummer jeweils zu korrelieren, wurden mit Hilfe eine Contact-Import-Tools Nummern geprüft, um zu sehen, ob diese mit einem Facebook-Account verbunden waren. Auf dem Profil des Nutzers wurde dieser dann besucht und von dort wurden die öffentlichen Daten gescrapt („abgeschöpft“). Anfang April 2021 wurde durch die Medien berichtet, dass Daten von ca. 533 Millionen Nutzern der Plattform der Beklagten aus 106 Ländern im Internet veröffentlicht wurden.

9
Beim Anlegen eines Facebook-Accounts wird der künftige Nutzer auf Datenschutz- und Cookie- Richtlinien hingewiesen. Diese sind durch eine Verlinkung getrennt abrufbar. Nach der Anmeldung sind zunächst die

Vor- bzw. Standardeinstellungen aktiviert. Demnach können „alle“ Personen sehen, welche Seiten der Nutzer abonniert oder mit wem er befreundet ist. Ebenso können „alle“ den neuen Nutzer über seine E-Mail-Adresse „finden“. Die Angabe der Mobilfunknummer ist nicht grundsätzlich zwingend. Wenn der Nutzer die Zweifaktor-Authentifizierung nutzen möchte, ist die Angabe einer Mobilfunknummer jedoch zwingend. Entscheidet sich ein Nutzer, diese anzugeben, kann er in den Suchfunktionen einstellen, in welchem Umfang er über diese gefunden werden will. Der Nutzer kann die Einstellungen individuell verändern und im Hilfebereich einlesen, wie die Beklagte insbesondere die Mobilfunknummer verwendet.

10
2. Als streitig behandelt hat das Landgericht folgendes Klägervorbringen:

11
Die Beklagte habe gegen zahlreiche Vorschriften der Datenschutzgrundverordnung verstoßen, nämlich

(a) entgegen Art. 4 Nr. 2 DSGVO Daten des Klägers ohne Rechtsgrundlage und ohne ausreichende Informationen verarbeitet,

(b) entgegen Art. 5 ff. DSGVO Daten des Klägers unbefugt Dritten zugänglich gemacht,

(c) ferner Art. 15 (Auskunft), 17 (Löschung) und 18 (Verarbeitungsrestriktion) DSGVO verletzt:

12
Im April 2021 seien Daten auch des Klägers im Internet veröffentlicht worden. Die Beklagte habe keine hinreichenden Sicherheitsvorkehrungen gegen einen unbefugten Zugriff Dritter getroffen. Ferner seien ihre Einstellungen bzgl. der Telefonnummer des Klägers so konzipiert, dass keine echte Sicherheit möglich sei.

13
Von dem Scraping-Vorfall seien auch die Daten des Klägers betroffen. Dem Kläger sei durch die unbefugte Veröffentlichung seiner personenbezogenen Daten ein Schaden entstanden, der darin bestehe, dass der Kläger

(a) einen erheblichen Kontrollverlust über seine Daten erlitten habe und

(b) in einem Zustand großen Unwohlseins und Sorge über möglichen Missbrauch seiner Daten verbleibe.

(c) Der Kläger habe seit 2021 vermehrt dubiose E-Mails und SMS-Nachrichten von unbekannten Adressen und Nummern erhalten.

14
3. Das Landgericht ist dem mit folgender Begründung nicht gefolgt:

15
3.1 Der Kläger könne keinen immateriellen Schaden aus § 82 Abs. 1 DSGVO zu (Klageantrag Ziff. 1) ersetzt verlangen.

16
Der Schutzbereich des Art. 82 DSGVO sei nicht eröffnet mit Blick auf die hier behaupteten Verstöße gegen Informationspflichten (Artt. 13, 14, 15, 24, 25 und Art. 34 DSGVO).

17
Erstens sei Anknüpfungspunkt für eine Haftung nach Art. 82 DSGVO stets eine der Verordnung nicht entsprechende Verarbeitung i.S.d. Art. 4 Nr. 2 DSGVO. Dies zeige auch Erwägungsgrund 146. Nicht erfasst sei eine Verletzung bloßer Benachrichtigungspflichten oder Informationsrechte.

18
Zweitens habe die Beklagte nicht gegen Normen der DSGVO verstoßen.

19
3.1.1 Ein Verstoß gegen Art. 32 DSGVO (Sicherheit der Datenverarbeitung) liege nicht vor, da die Beklagte nicht verpflichtet gewesen sei, Schutzmaßnahmen zu treffen, damit die Erhebung von Informationen unterbleibt, die der Nutzer aufgrund seiner selbst gewählten Einstellung öffentlich zugänglich gemacht hat.

20

Da der Kläger eingestellt hatte, von allen („everyone“) über seine Telefonnummer („by phone number“) gefunden werden zu können, schließe das auch den Fall ein, dass Dritte den Kläger über seine Mobilfunknummer finden – auch wenn die Dritten hierzu elektronische Möglichkeiten zu Hilfe nehmen, indem sie etwa die Telefonnummern aus dem „Kontaktimporter“ der Plattform von Facebook hochladen, dann mit zufällig generierten anderen Telefonnummern vergleichen und so schließlich auf die Telefonnummer kommen, die der Kläger mit seinem Facebook-Konto verknüpft hat. Auch die unbekannten Dritten fielen unter den Begriff „everyone“.

21
Die „Verarbeitung“ der klägerischen Daten (Art. 4. Nr. 2 DSGVO) sei vorliegend unstreitig durch die „scrapenden“ Dritten geschehen. Die „gescrapten“ personenbezogenen Daten der Klagepartei seien für jedermann ohne Zugangskontrolle oder Überwindung technischer Zugangsbeschränkungen (z.B. Logins) abrufbar gewesen, und das habe der Kläger bereits durch die Anmeldung gewusst, aber die Entscheidung getroffen, sich öffentlich durch jedermann über seine Telefonnummer suchen zu lassen. Daran ändere sich nichts dadurch, dass der Kläger zugleich eingestellt hat, diese Telefonnummer solle nur ihm selbst angezeigt werden. Es bestehe somit keine Pflicht der Beklagten zu verhindern, dass die Telefonnummer des Klägers durch eine Suchfunktion gefunden wird.

22
3.1.2 Ein Verstoß gegen Art. 33 DSGVO liege nicht vor, da nach dieser Vorschrift die Beklagte lediglich verpflichtet sei, eigene Datenschutz-Verstöße der zuständigen Aufsichtsbehörde zu melden. Der Scraping-Vorfall sei aber, wie gezeigt, kein eigener Verstoß der Beklagten.

23
3.1.3 Auch ein Verstoß gegen Art. 35 DSGVO liege nicht vor: Soweit der Kläger der Beklagten vorwerfen wolle, keine zureichende Folgenabschätzung vorgenommen zu haben, so sei nicht ersichtlich, wie eine so verstandene Pflichtverletzung kausal geworden sein sollte für den Verlust über die Kontrolle der „gescrapten“ Daten. Gegen die Kausalität spreche bereits, dass diese Daten schon vorher öffentlich zugänglich waren aufgrund des Profils, das der Kläger der Plattform „Facebook“ angelegt hatte.

24
3.1.4 Auch gegen Art. 15 Abs. 1 a) c) DSGVO habe die Beklagte nicht verstoßen, sondern dem Kläger Auskunft gegeben (Anlage B 16) und dabei alle relevanten und ihr möglichen Angaben gemacht (Nutzer-ID, Vorname, Nachname, Land und Geschlecht). Der Anspruch sei durch Erfüllung erloschen (§ 362 Abs. 1 BGB). Die Frage, welchen Empfängern die Daten des Klägers durch Ausnutzung des „Kontakt-Import-Tools“ im Sinne des Art. 15 Abs. 1 c) DSGVO zugänglich gemacht wurden, habe die Beklagte nicht beantworten müssen, da sie das nicht konnte: Das „Scraping“ sei ja unstreitig das Werk unbekannter Dritter gewesen, und da die Daten auf „öffentlich“ gestellt waren, sei es auch nicht möglich, die Dritten zu ermitteln. Ebenso unmöglich sei der Beklagten die Angabe, wann (genau) die Daten „gescrapt“ wurden.

25
3.1.5 Es liege kein Verstoß gegen Art. 5 Abs. 1 DSGVO vor:

26
Der Beklagten könne weder ein Verarbeitungsfehler (Art. 5 Abs. 1 DSGVO) noch mangelnde Transparenz von Information und Aufklärung (Art. 12, 13, 14 DSGVO) vorgeworfen werden. Sie habe ihren Nutzern – und damit auch der Klägerseite – im streitgegenständlichen Zeitraum im Rahmen ihrer Datenrichtlinie und dem Hilfebereich in Bezug auf die Verwendung der Daten und insbesondere der Verwendung der Telefonnummer sowie der Kontakt-Import-Funktion klare Informationen zur Verfügung gestellt (Anlagen B 1-9), die verständlich und zugänglich waren.

27
Diese seien sinnvoll in mehreren Ebenen und mit verlinkten Einstellungsmöglichkeiten angelegt, und gäben Auskunft über sämtliche Nutzungs- und Suchbarkeitsoptionen, wie sich bereits in den Screenshots zeige, die der Kläger selbst vorgelegt hat. Der Nutzer werde sogleich darauf aufmerksam gemacht, dass er die Privatsphäre-Einstellungen individuell anpassen kann. Die Datenschutzinformationen seien unvermeidlich umfangreich, aber würden hierdurch nicht unübersichtlich

28
3.1.6 Auch gegen Art. 24, 25 Abs. 2 DSGVO habe die Beklagte nicht verstoßen.

29
Unstreitig habe die Beklagte das Nutzerprofil dergestalt voreingestellt, dass für die Registrierung nur der Name, das Geschlecht und die ID sichtbar sind und dies auch stets bleiben. Dem stimme aber jeder Nutzer zu, indem er die Datenschutzbestimmungen akzeptiert, bevor er sein Profil anlegt.

30
Soweit der Nutzer sich entschließt, seine Telefonnummer zu hinterlegen, was für die Registrierung bei Facebook „gerichtsbekannt nicht erforderlich“ sei, habe die Beklagte dies zwar als Suchbarkeits-Option voreingestellt (als „everyone“ „by phone number“). Ändere der Nutzer diese Einstellung nicht, so könne er zwar über seine E-Mail-Adresse und Mobilnummer gefunden werden (und folglich hierüber „Freundschaftsanfragen“ bekommen).

31
Aber hierüber werde der Nutzer, auch wenn er „technisch unkundig“ ist, durch entsprechende Begleithinweise der Beklagten informiert und über Einstellungsoptionen (insbesondere Begrenzungsmöglichkeiten) informiert.

32
Zudem gelte: Wer die Plattform eines sozialen Netzwerkes der von der Beklagten betriebenen Art nutzt, müsse sich mit deren Gepflogenheiten vertraut machen; vor diesen könne Art. 25 DSGVO ihn nicht „vollends“ schützen. Die hier interessierende Plattform sei schließlich angelegt „auf Kontaktsuche und das Finden von Kontakten“, wobei der Nutzer mitgeteilt bekommt, er müsse seine Telefonnummer nicht zwingend hinterlegen, werde aber, wenn er dies tue, leichter gefunden und könne die Plattform besser nutzen. Hier müsse jeder Nutzer selbst „eigenverantwortlich entscheiden, in welchem Umfang er diese Möglichkeiten nutzt und entsprechende Daten freigibt“.

33
Letztlich könne aber offenbleiben, ob die Beklagte gegen Art. 25 DSGVO verstoßen habe, denn bejahendenfalls folge daraus kein Schadensersatzanspruch des Nutzers nach Art. 82 Abs. 1 DSGVO, weil Art. 25 DSGVO rein „organisatorischen Charakters“ sei und bereits Wirkung entfalte, bevor die eigentliche Datenverarbeitung beginnt (Gola/Heckmann/Nolte/Werkmeister, 3. Aufl. 2022, DSGVO Art. 25 Rn. 3, 34; Kühling/Buchner/Hartung, 3. Aufl. 2020, DSGVO Art. 25 Rn. 31). Erst mit deren Beginn gelte die DSGVO (Art. 2 Abs. 1 DSGVO), nämlich wenn es tatsächlich zu einer Verarbeitung personenbezogener Daten kommt (Ehmann/Selmayr/Baumgartner, 2. Aufl. 2018, DSGVO Art. 25 Rn. 7). Ein Anspruch aus Art. 82 DSGVO komme daher nur in Betracht, wenn weitere DSGVO-Verstöße vorlägen (Gola/Heckmann/Nolte/Werkmeister, 3. Aufl. 2022, DSGVO Art. 25 Rn. 3).

34
3.1.7 Es liege auch kein Verstoß gegen Art. 6 Abs. 1, 13 Abs. 1 DSGVO vor.

35
Die Beklagte habe den Kläger ausreichend aufgeklärt gemäß Art. 13 Abs. 1 DSGVO, insbesondere über die Zwecke der Verarbeitung sowie deren Rechtsgrundlage und die etwaigen Empfänger oder Kategorien von Empfängern der personenbezogenen Daten.

36
Der Kläger habe zudem mit der Zustimmung zu den Nutzungsbedingungen und der Datenrichtlinie die Einwilligung zu der Verarbeitung der ihn betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben gemäß Art. 6 Abs. 1 S. 1 a) DSGVO.

37
Insbesondere gelte auch hier, das die Beklagte die Datenschutzrichtlinie sowie die Nutzungsbedingungen in einfach verständlicher Sprache abgefasst habe, zu denen der Kläger einen leichten Zugang hatte. Die Website der Beklagten weise den Nutzer sogar mehrfach darauf hin, dass man einen „Privatsphärecheck“ durchführen kann. Insoweit entspreche das Ersuchen der Einwilligung auch den Voraussetzungen des Art. 7 Abs. 2 DSGVO.

38
3.1.8 Der Kläger habe auch den Eintritt eines Schadens im Sinne des Art. 82 Abs. 1 DSGVO nicht bewiesen.

39
Der (nach Erwägungsgrund 146 S. 3 weit zu verstehende) Schadensbegriff, dem auch „Abschreckungscharakter“ zukomme, setze gleichwohl einen „erlittenen“ Schaden (Erwägungsgrund 146) voraus, der sonach „tatsächlich entstanden“ sein müsse. Bloße Befürchtungen fielen hierunter nicht, so dass ein bloßer Verstoß gegen die DSGVO bei der Datenverarbeitung für einen Anspruch auf Ersatz immaterieller Schäden nicht ausreicht. Vielmehr müsse der Verstoß kausal zu einer spürbaren Beeinträchtigung geführt haben z.B. eine „Bloßstellung“ (OLG Brandenburg, Beschluss vom 21.06.2021, 1 U 69/20 = BeckRS 2021).

40
Der Kläger habe hier, schon wenn man seinen Angaben (insbesondere bei der persönlichen Anhörung) folge, keinen Schaden erlitten.

41
(a) Ein bloßer Kontrollverlust über seine Daten sei keine spürbare Beeinträchtigung im Sinne einer Persönlichkeitsverletzung und damit kein Schaden.

42
(b) Soweit der Kläger einen „Zustand erhöhten Misstrauens“ hatte vortragen lassen, widerlege er das selbst durch seine informatorischen Angaben im Termin, denen zufolge er weiterhin bei Facebook und weiteren sozialen Plattformen angemeldet ist und sensible Daten, wie z.B. seine Handynummer, auch einem bekannten Internetversandhändler hinterlegt hat. Dies sei nicht vereinbar mit der Annahme eines Gefühls von „Stress, Misstrauen, Angst vor Kontrollverlust etc“.

43
(c) Soweit der Kläger vortrage, Anrufe unbekannter Nummern und/oder Spamnachrichten erhalten zu haben, könne das nicht kausal auf den „Scraping-Vorfall“ zurückgeführt werden. Denn insoweit ergebe sich aus den Angaben des Klägers bei seiner Anhörung, dass er die Spam-Nachrichten im Zusammenhang mit seinem Konto bei dem o.g. Versandhändler erhalte. Dort unterhalte der Kläger jedoch ein Kundenkonto mit dort hinterlegter Handynummer. Die Spamnachrichten könnten hiernach ohne weiteres auch auf das Nutzerverhalten des Klägers beim Versandhändler zurückzuführen sein.

44
3.2 Auch nach nationalem Recht stehe dem Kläger der geltend gemachte Zahlungsanspruch nicht zu.

45
Ein vertraglicher Anspruch gemäß §§ 280 Abs. 1, 241 Abs. 2 BGB scheide aus, weil der Kläger keine Verletzung von vertraglichen Pflichten durch die Beklagte dargelegt habe.

46
Ansprüche gemäß §§ 823 Abs. 1, 253 Abs. 2 BGB i.V.m. dem allgemeinen Persönlichkeitsrecht bzw. mit dem Recht auf informationelle Selbstbestimmung (vgl. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) bestünden nicht, da der Kläger keine Verletzung eines der in § 253 Abs. 2 BGB genannten Rechtsgüter darlege.

47
Schließlich bestehe auch kein Anspruch nach § 823 Abs. 2 BGB i.V.m. den Vorschriften der DSGVO (s.o.)

48
3.3 Aus obigen Gründen könne der Kläger auch die mit Klageantrag Ziff. 2 verfolgte Feststellung nicht verlangen.

49
3.4 Der Kläger habe auch keinen Unterlassungsanspruch (Klageantrag. Ziff. 3).

50
Es fehle an der für den Unterlassungsanspruch nötigen Erstbegehung. Die Beklagte habe weder gegen Sicherungspflichten verstoßen (Antragsteil 3. A), noch den Kläger fehlerhaft aufgeklärt (Antragsteil 3.b).

51
3.5 Der Auskunftsantrag (Klageantrag Ziff. 4) sei unbegründet.

52

Auskunftsansprüche nach Art. 15 Abs. 1 DSGVO habe die Beklagte durch ein vorgerichtliches Schreiben (Anlage B16) bereits erfüllt.

III.-

53
Die Berufungsbegründung bringt vor:

54
1. Der Anwendungsbereich von Art. 82 DSGVO sei entgegen der Auffassung des Landgerichts eröffnet, weil der Verantwortliche hiernach für jeglichen – formellen wie materiellen – Verstoß gegen die DSGVO hafte, sofern dem Betroffenen ein Schaden daraus entstanden ist (BerBegr S. 9/12), nicht nur für Fehler bei der Verarbeitung. Auch der Begriff der „Verarbeitung“ sei weit zu verstehen.

55
2. Die Beklagte habe gegen Art. 5 Abs. 1 DSGVO verstoßen, nämlich dem Kläger nicht die Möglichkeit geboten, „in informierter Art und Weise über die Verarbeitung“ der ihn betreffenden Daten „zu entscheiden“. Die Informationen hierzu seien mehrschichtig verschachtelt und dadurch nicht transparent, denn es müsse bedacht werden, dass Nutzer ein Konto „mit Billigung der AGB und Datenschutzinformationen innerhalb weniger Klicks“ erstellen (BerBegr S. 13). Dass der Nutzer stattdessen seine Einstellungsmöglichkeiten erst einmal „über mehrere Links und Unterlinks“ erschließen könne, laufe der Transparenz zuwider (Ber Begr. S. 14).

56
3. Die Beklagte habe gegen Art. 32 DSGVO verstoßen.

57
Das meine auch die irische Aufsichtsbehörde, die hierwegen ein Bußgeld verhängt habe (BerBegr S. 14).

58
Es fehle an einer datenschutzfreundlichen Voreinstellung. Dies zu ändern, sehe ein Nutzer keinen Anlass (BerBegr. S. 16), weil die Beklagte für „weitere Informationen zur Förderung der Sicherheit“ auf den „Hilfebereich“ unter „Sicherheit“ verweise und damit dem Nutzer suggeriere, dass diese „Sicherheit“ bereits ohne weiteres gegeben sei. Die Voreinstellungen der Beklagten in eine datenschutzfreundlichere Richtung anzupassen, sei dem Nutzer nicht zumutbar (BerBegr. S. 18).

59
Die Beklagte sei darlegungs- und beweisbelastet, wenn sie behaupten wolle, die geeigneten technischen und organisatorischen Maßnahmen zur wirksamen Umsetzung der Datenschutzgrundsätze (Art. 25 Abs. 2 DSGVO) ergriffen zu haben (BerBegr S. 15/18) einschließlich regelmäßiger Evaluierung und Kontrolle (BerBegr S. 19). Die Zustimmung des Klägers zur „Datenschutzrichtlinie“ der Beklagten – einer Sammlung von Allgemeinen Geschäftsbedingungen – verstoße gegen §§ 309 Nr. 12 b) und 308 Nr. 6 BGB. Deshalb könne die vom Kläger erteilte Zustimmung diesem „nicht zum Nachteil gereichen“ (BerBegr s. 19).

60
Die Beklagte habe die Gefährlichkeit des Contact-Import-Tools erkennen müssen:

61
Der hier interessierende Scraping-Vorfall verstoße gegen die Nutzungsbedingungen der Beklagten, weil das Contact-Import-Tool nur dazu dienen soll, persönliche Kontakte[, die der Suchende selbst schon besitzt, auch] auf Facebook aufzufinden. Der Missbrauch bestehe darin, dass die unbekannten Dritten das Contact-Import-Tool dazu herangezogen hätten, vorgegebenen Telefonnummern jeweils Facebook-Profile zuzuordnen, bei denen der jeweilige Nutzer seine Telefonnummer angegeben hatte, wenngleich diese auf Facebook nicht öffentlich einsehbar gewesen sei (BerBegr S. 20). Die Dritten hätten so in Erfahrung gebracht, wer hinter der ihnen bereits bekannten Telefonnummer steht, und seien so auch an die weiteren Informationen gekommen, die zu der Person auf Facebook veröffentlicht sind. Den Telefoninhaber bringe das in die Gefahr, dass alle seine zusammengetragenen Daten veröffentlicht und dabei die Telefonnummer nunmehr zusammen mit dem Namen veröffentlicht werde. So könne der Nutzer zum Opfer von „gezielten Phishing-Attacken, Identitätsdiebstahl und weiterem Missbrauch der Daten“ werden. Dem Opfer drohe der „Eintritt von materiellen oder immateriellen Schäden“ (BerBegr S. 20). Dass „Scraping“ weit verbreitet ist, sei der Beklagten klar gewesen. Deshalb habe sie „Maßnahmen für ein angemessenes Schutzniveau für die

personenbezogenen Daten hinsichtlich des Risikos von Scraping“ treffen müssen (BerBegr S. 20), und zwar präventiv (BerBegr S. 21) und nicht erst nach dem Vorfall.

62
4. Die Beklagte habe gegen Art. 24 und 25 DSGVO verstoßen, indem sie die Voreinstellungen

- in der Zielgruppenauswahl auf „alle“ gesetzt und

- in den Suchbarkeits-Einstellungen eine Angabe der Telefonnummer vorgesehen hat,

während nach dem Grundsatz „privacy by default“ (statt „privacy by design“) gelten müsse, dass immer diejenigen Voreinstellungen zu wählen sind, die am wenigsten an Verwendung von Nutzerdaten erwarten lassen.

63
Wenn die Voreinstellungen dahin gehen, dass jeder Nutzer mit einem anderen über die Telefonnummer verbunden „bzw.“ aufgefunden werden kann, so würden – entgegen Art. 25 Abs. 2 S. 3 DSGVO die Daten einer „unbestimmten Zahl von natürlichen Personen zugänglich gemacht“ (BerBegr S. 22). Das sei mit Art. 25 Abs. 2 S. 3 DSGVO nur dann vereinbar, wenn es der Nutzer selbst ist, der durch sein „Eingreifen“ diese Daten zugänglich macht. Das eigene „Eingreifen“ des Nutzers sei aber nur dann anzunehmen, wenn die Voreinstellungen im ersten Schritt die Preisgabe an den unbestimmten Personenkreis verhindern und es dem Nutzer lediglich freisteht, diese Preisgabe durch aktive Änderung der Einstellungen selbst herbeizuführen (BerBegr S. 23/26).

64
Die Voreinstellungen der Beklagten seien auch nicht damit zur rechtfertigen, dass deren Unternehmenszweck nun einmal darin besteht, Menschen mit ähnlichen Interessen zusammenzubringen (BerBegr S. 21): Hierfür sei es nämlich nicht nötig, dass der Nutzer sich über seine Telefonnummer suchbar macht. Wer die Telefonnummer des Nutzers bereits habe, könne den Nutzer anrufen, um Kontakt mit ihm zu haben und sich mit ihm nachfolgend auch auf Facebook zu treffen. So gesehen sei es „obsolet“, anhand der Telefonnummer den Facebook-Account aufspüren zu wollen. Diese Möglichkeit (= Suchbarkeit über die Telefonnummer) und das Contact-Import-Tool seien somit für die eigentlichen Zwecke von Facebook nicht von nennenswerter Bedeutung, andererseits aber ein Einbruchstor für Missbrauch, wie der Scraping-Vorgang aufgezeigt habe (BerBegr. S. 22/26).

65
5. Die Beklagte habe gegen ihre Aufklärungs- und Informationspflichten nach Art. 13, 14 DSGVO verstoßen.

66
Diese Pflichten entstünden nicht erst mit der Verarbeitung, sondern schon mit der Erhebung der Daten (BerBegr. S. 26/17). Die Beklagte habe angegeben, dass die Telefonnummer zum Zweck der so genannten „Zwei-Faktor-Authentifizierung“ im Interesse besonderer Sicherheit verarbeitet werde. Sie habe es versäumt, den Kläger darüber aufzuklären, dass die Telefonnummer für das Contact-Import-Tool verwendet werden soll (BerBegr S. 27).

67
Das Contact-Import-Tool ermögliche es, dass der Facebook-Nutzer seine auf dem eigenen Smartphone gespeicherten Telefonnummern mit den auf Facebook gespeicherten Nutzerprofilen darauf abgleichen kann, welcher seiner bestehenden Smartphone-Kontakte ebenfalls ein Konto auf Facebook hat, das mit der jeweils im Smartphone gespeicherten Telefonnummer verknüpft ist (BerBegr S. 28). Anschließend könne der suchende Nutzer das so aufgefundene fremde Facebook-Nutzerprofil „als ‚Freund‘ hinzufügen“ (BerBegr S. 28).

68
Diese Funktion beschreibe die Beklagte aber nicht in ihren „Datenrichtlinien“ (BerBegr S. 28); sie liefere keinen Hinweis, dass die Telefonnummer des Nutzers für das „Contact-Import-Tool“ benutzt wird (BerBegr s. 28). Darüber kläre die Beklagte auch nicht „unter den ‚Handy-Einstellungen‘ sowie den diesbezüglichen Untermenüs“ auf und schildere es auch nicht im „Hilfebereich“ (BerBegr S. 28), wobei es auf diesen ohnehin nicht ankomme, da der Nutzer den „Hilfebereich“ erst erreichen kann, wenn seine Daten bereits erhoben sind, und zwar einschließlich der Telefonnummer, die der Nutzer entweder bei der Registrierung oder diese

bei Abarbeitung der „Handy-Einstellungen“ eingegeben haben kann (BerBegr S. 29). Der „Hilfebereich“ leiste somit eine etwaige Aufklärung nicht „bei Erhebung“ der Daten.

69
6. Die Beklagte habe gegen Art. 33, 34 DSGVO verstoßen. Die Meldung an die Aufsichtsbehörde und die Benachrichtigung des Klägers seien veranlasst gewesen, da die Beklagte zuvor die o.g. Verstöße begangen habe (BerBegr S. 29/35). Der Verstoß der Beklagten liege bereits darin, dass Dritte massiv gegen die Richtlinien der Beklagten verstoßen haben, denn das sei eine „Verletzung der Sicherheit“, die auch bei „Zweckentfremdung von Daten“ anzunehmen sei und zu einer „Verletzung der Vertraulichkeit“ geführt habe (BerBegr S. 30), nämlich allein schon durch das Ausmaß des Scrapings (BerBegr S. 31).

70
7. Die Beklagte habe gegen Art. 35 DSGVO verstoßen. Die unstreitig unterbliebene Datenschutz-Folgenabschätzung sei „mitursächlich für die vorliegenden Schäden der Klägerseite“ geworden.

71
8. Die Beklagte habe gegen Art. 15 DSGVO verstoßen.

72
Die Beklagte sei unstreitig „bereits gegen einfache Scraper vorgegangen“. Desto weniger könne sie erklären, warum sie im vorliegenden Fall dem Kläger nicht „Ross und Reiter“ nennen wolle, d.h. nicht mitteile, an welche Empfänger die Daten gegangen seien (BerBegr S. 36). Der Kläger habe vorgetragen, dass der Empfänger mittels so genannter „Logfiles“ nachzuverfolgen sei. Dem habe die Beklagte nichts entgegengesetzt, so dass das Landgericht nicht einfach habe annehmen dürfen, weitere Auskünfte seien der Beklagten unmöglich.

73
9. Zu Unrecht verneine das Landgericht einen ersatzfähigen Schaden.

74
Angesichts des weiten Schadensbegriffs könne keine Erheblichkeitskontrolle geboten sein (BerBegr S. 40/42).

75
(a) Der Kontrollverlust sei bereits ein Schaden (BerBegr S. 42/50); das zeige bereits Erwägungsgrund 85. Deshalb habe das Landgericht keinen Anlass gehabt, den Kläger dazu anzuhören, ob er einen Kontrollverlust befürchte, denn der sei ohnehin eingetreten.

76
(b) Den weiteren Schaden des Klägers „durch Ärger, Angst, Stress, Sorge“ habe der Kläger bei seiner Anhörung bestätigt, indem er schilderte, seit dem Datenleck Kontaktversuche von unbekannten Dritten in Form von „Spam“-SMS und „Spam“-Anrufen erhalten zu haben.

77
Als Auswirkung von Ängsten, Stress sowie Komfort- und Zeiteinbußen sei der Umstand erkennbar, dass der Kläger sich „mit dem Datenleak und der Herkunft der Daten auseinandersetzen musste“ (BerBegr S. 43). Diese Auseinandersetzung wiederum sei „geeignet, zu einem belastenden Eindruck des Kontrollverlusts zu führen“, verschlimmert dadurch, dass die benannten Daten „in Kombination sogar im sog. Darknet gehandelt“ würden (Ber Begr S. 43). Schon im „möglichen Kontrollverlust“ (BerBegr S. 44) sei ein Schaden zu sehen.

78
Der Kläger gebe seine Telefonnummer „stets bewusst und zielgerichtet weiter“ und mache sie „nicht wahl- und grundlos der Öffentlichkeit zugänglich, wie etwa im Internet“.

79
10. Zu Unrecht versage das Landgericht die flankierende Feststellung einer Ersatzpflicht für künftige Schäden.

80

Diese sei schon deshalb gerechtfertigt, weil das Landgericht einen Schaden hätte annehmen müssen (BerBegr S. 56). Aber selbst wenn man meine, ein Schaden sei noch nicht eingetreten, so seien künftige Schäden möglich, und das genüge (BerBegr S. 56, BGH, 29.6.2021 – VI ZR 52/18). So sei denkbar, dass der Kläger sich in der Zukunft gezwungen sähe, sich eine neue Mobiltelefonnummer zu beschaffen oder den Anbieter zu wechseln, was Kosten verursachen werde. Schäden seien zu erwarten, falls der Kläger überlistet werde durch Anrufer, denen er mit „ja“ antwortet oder durch Anklicken von Links, die er per SMS erhalte [von unlauteren Dritten, die die gescrapten Daten verwendet haben, um den Kläger zu erreichen] (BerBegr S. 57) oder durch eine ganze Palette telefonischer oder computergestützter Trickbetrugs-Maschen (im Einzelnen BerBegr S. 58/60).

81
11. Zu Unrecht versage das Landgericht den Unterlassungsanspruch (BerBegr S. 60/66)

82
Dieser folge aus §§ 280 Abs. 1, 241 Abs. 2 BGB, ergebe sich daneben aber auch aus „§ 1004 BGB analog, §§ 823 Abs. 2, 1004 BGB“ (BerBegr S. 61), den Art. 79 DSGVO weder sperre noch einschränke.

83
Die Wiederholungsgefahr bestehe ungeachtet dessen, dass der Kläger die Einstellungen von „alle“ auf „nur ich“ zurücksetzen kann und die Beklagte die Suchbarkeitsfunktion deaktiviert hat (BerBegr S. 62) oder haben will (BerBegr S. 64) sowie „Anti-Scraping-Maßnahmen“ vorhält (BerBegr S. 62), mit denen sie ein eigenes Team betraut hat (BerBegr S. 64). Denn die Wiederholungsgefahr werde indiziert durch die Rechtsverletzungen und sei beklagtenseits nicht widerlegt (BerBegr S. 62/63). Dazu brauche es im Regelfall eine vertragsstrafbewehrte Unterlassungserklärung.

84
Eine Einstellungsänderung (von „everyone“ auf „friends of friends“) bringe jedenfalls keine Abhilfe, denn gescrapt worden seien auch Daten von Nutzern, die nicht „everyone“ eingestellt hatten (BerBegr S. 64/65).

85
12. Zu Unrecht versage das Landgericht den Auskunftsanspruch (BerBegr S. 65/67).

86
Es fehle vorliegend die Angabe des Empfängers der gescrapten Daten.

87
13. Aus denselben Gründen hätte das Landgericht nach nationalen Vorschriften Schadensersatz ausurteilen müssen (BerBegr. S. 67).

IV.

88
Die Berufung ist ohne Erfolgsaussicht.

89
Das strukturiert begründete Urteil des Landgerichts leidet nicht an Rechtsfehlern (§ 546 ZPO). Die zugrunde zu legenden Tatsachen (§ 529 ZPO) gebieten keine andere Entscheidung (§ 513 Abs. 1 ZPO).

90
1. Zutreffend versagt das Landgericht einen Schadensersatzanspruch.

91
Das Ersturteil arbeitet überzeugend heraus, dass der Beklagten eine schadenskausale Pflichtverletzung, die in den Anwendungsbereich des Art. 82 DSGVO fiele, nicht angelastet werden kann; auf die diesbezüglichen Ausführungen des Landgerichts ist Bezug zu nehmen.

92
Ihnen ist hier lediglich hinzuzufügen: Insbesondere einen Verstoß gegen Art. 32 durch „zu weite“ Voreinstellungen musste das Landgericht nicht annehmen. Art. 32 DSGVO schreibt nicht schlechthin datenschutzfreundliche Voreinstellungen vor, sondern gebietet – wesentlich allgemeiner gehalten – „geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“. Das ist bei einer Kontaktplattform auch dadurch möglich, dass dem Nutzer durch

Anleitungen und Hilfen die Möglichkeit gegeben wird, die Einstellungen enger zu fassen und zudem einen „Privacy-Check“ durchzuführen.

93
Anderes ergibt sich auch nicht etwa aus Erwägungsgrund 78 zur DSGVO, denn dort werden datenschutzfreundliche Voreinstellungen lediglich als Beispiel für Schutzmaßnahmen genannt, die je nach Sachlage und Zusammenhang empfehlenswert seien.

94
Er lautet:

„Zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten natürlicher Personen ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen dieser Verordnung erfüllt werden. Um die Einhaltung dieser Verordnung nachweisen zu können, sollte der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun. Solche Maßnahmen könnten unter anderem darin bestehen, dass die Verarbeitung personenbezogener Daten minimiert wird, personenbezogene Daten so schnell wie möglich pseudonymisiert werden, Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird, der betroffenen Person ermöglicht wird, die Verarbeitung personenbezogener Daten zu überwachen, und der Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern. In Bezug auf Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen. Den Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sollte auch bei öffentlichen Ausschreibungen Rechnung getragen werden“.

95
Das Landgericht durfte hier berücksichtigen, dass Facebook eine Plattform für Nutzer ist, die sich in erster Linie „finden lassen“ wollen, um sogenannte „Freundschaftsanfragen“ zu erhalten, wobei der Begriff „Freundschaft“ hier nicht in dem engen Sinne zu verstehen ist, der die deutsche Sprachtradition prägt. Als „technische und organisatorische Maßnahme“ durfte es das Landgericht in diesem Zusammenhang als ausreichend ansehen, dass die Nutzer hier das Ausmaß der Findbarkeit selbst einstellen konnten, angeleitet durch transparente Hilfen und Erklärungen, die umfangreich, aber verständlich und sinnvoll gegliedert sowie zugänglich waren.

96
2. Das kann indessen dahinstehen, da im vorliegenden Einzelfall auch kein Schaden im Rechtssinne eingetreten ist.

97
Das Landgericht hat unter zutreffender Einwertung von Erwägungsgrund 146 herausgearbeitet, dass der Schadensbegriff zwar im Prinzip weit reicht, aber eine fühlbare reale Beeinträchtigung voraussetzt. An dieser fehlt es hier, wie das Landgericht anhand der persönlichen Anhörung des Klägers herausgearbeitet hat. Was die Berufungsbegründung hiergegen erinnert, überzeugt nicht:

98
(a) Erwägungsgrund 85 besagt nicht, dass jeder Kontrollverlust ein Schaden ist.

99
Er lautet in seinem Satz 1, den die Berufung hier offensichtlich anzieht:

„Eine Verletzung des Schutzes personenbezogener Daten kann – wenn nicht rechtzeitig und angemessen reagiert wird – einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer

Rechte, Diskriminierung, Identitätsdiebstahl oder betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person“.

100
(b) Dass der Kläger „durch Ärger, Angst, Stress, Sorge“ geplagt sei, hat die Anhörung nicht ergeben, sondern seinen freimütigen Angaben war u.a. zu entnehmen, dass er die Plattform weiter nutzt, was dem Landgericht zeigte, dass der Kläger nicht durchgreifend bekümmert ist. Was er an Zeit und Kraft aufgewendet habe, um sich mit dem Problem auseinanderzusetzen, war nicht in der Weise greifbar geworden, dass ein „erlittener“ Schaden darin gesehen werden musste.

101
(c) Dass der Kläger seit dem Datenleck Kontaktversuche von unbekannten Dritten in Form von „Spam“-SMS und „Spam“-Anrufen erhalten habe, hat der Kläger dahin relativiert, diese beruhten wahrscheinlich darauf, dass er seine Mobiltelefonnummer bei dem mehrfach erwähnten großen und weltweit tätigen Versandhandelsunternehmen hinterlegt habe. Das Landgericht hatte daher verständlicherweise unüberwindliche Bedenken, die SMS und Anrufe gerade der Beklagten als kausal verursachten Schaden anzulasten.

102
2. Nicht zu beanstanden ist ferner, dass das Landgericht auch für einen zukünftigen Schaden keine Anhaltspunkte sah.

103
3. Zutreffend versagt das Landgericht den Unterlassungsanspruch

104
Die Wiederholungsgefahr besteht bereits deshalb nicht, weil der Kläger die Einstellungen von „alle“ auf „nur ich“ zurücksetzen kann. Das erfordert keine weiteren Maßnahmen der Beklagten, so dass offen bleiben kann, ob diese die Suchbarkeitsfunktion deaktiviert hat und „Anti-Scraping-Maßnahmen“ ins Werk gesetzt hat.

105
Denn selbst wenn eine Rechtsverletzung vorläge, die – grundsätzlich – Wiederholungsgefahr zu indizieren geeignet wäre, wäre diese Indizwirkung durch obige Fallumstände hier widerlegt.

106
Nicht verfangen kann der Einwand, wonach es keine Abhilfe bringe, wenn der Kläger seine Einstellungen von „everyone“ auf „friends of friends“ umstellt. Es mag unterstellt werden, dass auch Daten von Nutzern „gescrapt“ worden sind, die – anders als der Kläger – nicht „everyone“ eingestellt hatten. Das ist aber nicht der Schadenshergang, der vorliegend anzunehmen war und an dem die Wiederholungsgefahr zu messen wäre. Dass sich der hier festgestellte Schadenshergang wiederholen würde, kann der Kläger schon durch die geänderten Einstellungen bewirken. Stellt er die Einstellungen von „alle“ auf „nur ich“ zurück, und würden seine Daten dann (erneut) gescrapt, so wäre das ein anderer Schadenshergang.

107
4. Zutreffend versagt das Landgericht den Auskunftsanspruch.

108
Anders als in den von der Berufungsbegründung angezogenen Entscheidungen anderer Gerichte (BerBegr S. 65/66) war der Auskunftsanspruch vorliegend erfüllt mit Ausnahme einer Angabe, wer der/die Scraper/in gewesen ist. Letztere Angabe (des „Empfängers“) kann die Beklagte nicht machen, weil sie den Empfänger nicht kennt. Dass sie in früheren Fällen gegen unbefugte Dritte vorgegangen ist, ändert hieran fallbezogen nichts.

109
5. Nach alledem hat das Landgericht auch Schadensersatzansprüche nach nationalem Recht zutreffend versagt.

C.- Frist:

110
Hierzu kann sich die berufungsführende Seite, soweit noch beabsichtigt, äußern bis zum 10.10. 2023.

111
Die Berufungsgegnerin braucht vorerst nicht zu erwidern.

112
Da die Berufung keine Aussicht auf Erfolg hat, legt das Gericht aus Kostengründen die Rücknahme der Berufung nahe. Im Falle der Berufungsrücknahme ermäßigen sich vorliegend die Gerichtsgebühren von 4,0 auf 2,0 Gebühren (vgl. Nr. 1222 des Kostenverzeichnisses zum GKG).