Landgericht Bochum, 5 O 334/23

Datum:	15.05.2024
Gericht:	Landgericht Bochum
Spruchkörper:	5. Zivilkammer
Entscheidungsart:	Urteil
Aktenzeichen:	5 O 334/23
ECLI:	ECLI:DE:LGBO:2024:0515.5O334.23.00

Rechtskraft: rechtskräftig

Tenor:

1. Die Klage wird abgewiesen.

2. Die Kosten des Rechtsstreits trägt der Kläger.

3. Das Urteil ist vorläufig vollstreckbar gegen Sicherheitsleistung in Höhe von

   120 % des jeweils zu vollstreckenden Betrages.

Tatbestand 1

Der Kläger macht gegen die Beklagte Ansprüche wegen behaupteter Datenschutzverstöße geltend. 2

Die Beklagte ist die Betreiberin der Internet-Plattform „G..com" sowie der Dienste auf jener Internetseite. Bei dieser Plattform handelt es sich um eine Social-Media-Plattform, welche dem Nutzer dazu dienen soll, mit Freunden und Bekannten insbesondere zu kommunizieren, Fotos zu teilen und sich mit anderen Nutzern auszutauschen. Entsprechend ermöglicht es die Plattform den Nutzern, persönliche Profile für sich zu erstellen und diese mit anderen Nutzern zu teilen. Im Zuge dieser persönlichen Profile können die Nutzer verschiedene Angaben zu ihrer Person tätigen. 3

Bei dem Anlegen eines Profils wird der künftige Nutzer auf die jeweils geltenden Datenschutz- und Cookie-Richtlinien hingewiesen. Zudem muss er seinen Vor- und Nachnamen und das Geschlecht angeben. Diese Daten sowie eine von W. erstellte Benutzer-ID sind als "immer öffentliche Nutzerinformationen" stets öffentlich auf dem eigenen 4

Nutzerprofil zu finden, d.h. auch von Personen, die selbst über kein eigenes Profil verfügen. Der Veröffentlichung dieser Daten muss bei Registrierung zugestimmt werden.

Darüber hinaus kann der jeweilige Nutzer freiwillig eine Vielzahl weiterer Angaben tätigen. Hinsichtlich dieser Angaben kann jeder Nutzer in den Einstellungen seines Profils in einem von der Beklagten vorgegebenen Rahmen festlegen, welche Daten von wem einsehbar sind (sog. Zielgruppenauswahl). Dabei kann gewählt werden, ob Daten nur für den jeweiligen Nutzer selbst, befreundete Nutzer, ggf. auch deren Freunde oder für alle, d.h. öffentlich zugänglich, sein sollen. 5

Datenpunkte wie „Land“, „Bundesland“, „Anschrift“, „Biografie“, „Standortdaten“, „Orte“, „Berufe“ oder „weitere korrelierende Daten“ entsprechen hingegen nicht den Profilfeldern bei W.. 6

Im Hilfebereich kann eingesehen werden, wie W. die jeweiligen Daten verwendet. 7

Ferner kann der Nutzer über seine konkreten persönlichen Profileinstellungen bestimmen, wer sein Profil im Rahmen einer Suchanfrage z.B. über die hinterlegte Telefonnummer oder E-Mail-Adresse finden kann (‘sog. Suchbarkeitsauswahl‘) 8

In dem streitgegenständlichen Zeitraum war es potenziell möglich, Nutzer anhand einer Telefonnummer zu finden, wenn ihre Einstellung betreffend die Telefonnummer auf „Alle“ eingestellt war. Neben der Option „Alle“ konnten Nutzer in den Privatsphäre-Einstellungen festlegen, dass nur „Freunde von Freunden“ oder „Freunde“ ihr Profil auf diese Art finden können. 9

Ab Mai 2019 stand Nutzern auch die Option „Nur ich“ zur Verfügung, mit der verhindert wird, dass irgendjemand anders das entsprechende Profil so finden kann. Die Grundeinstellung geht zunächst von einer Suchbarkeit für alle anderen Nutzer aus. Für alle Informationen, die ein Nutzer in sein Profil einträgt, ist die Voreinstellung „öffentlich“ standardmäßig ausgewählt. Diese Einstellungen hatte auch der Kläger so belassen. 10

Die Angabe der Mobilfunknummer ist für die Anmeldung nicht zwingend, kann jedoch für eine Zwei-Faktor-Authentifizierung verwandt werden. Insofern kann jeder Nutzer ebenfalls die Sichtbarkeit seiner Mobilfunknummer nach dem o.g. Schema festlegen, d.h. es ist sowohl möglich, die Sichtbarkeit für alle anderen Nutzer auszuschalten, als auch sie öffentlich einsehbar zu belassen. 11

Unabhängig davon verfügte die Plattform während des relevanten Zeitraums über eine Funktion, die es Nutzern ermöglichte, in den Adressbüchern ihres eigenen Mobilgerätes gespeicherte Rufnummern mit den bei W. hinterlegten Rufnummern anderer Nutzer abgleichen zu lassen. Sofern eine Übereinstimmung festgestellt wurde, wurde das zugehörige Profil angezeigt und dem Nutzer so die Kontaktaufnahme mit der ihr bekannten Person ermöglicht (sog. contact importer tool = CIT). 12

Das Kontakt-Import-Tool ist im Zusammenhang mit der W.-Mobile-App zu betrachten. Mithin werden die beiden Anwendungen für Smartphones bereitgestellt, insbesondere für solche mit dem Betriebssystem „L.". 13

Das Smartphone bietet die Möglichkeit, bestehende Kontaktdaten zusammengefasst in einem Adressbuch zu hinterlegen. Durch das Kontakt-Import-Tool ist es dem jeweiligen Anwender möglich, automatisiert die Informationen aus dem hinterlegten Adressbuch über 14

die W.-Mobile-App hochzuladen. Freunde und Bekannte können so auf W. identifiziert werden, indem abgefragt wird, ob die im Adressbuch hinterlegte Telefonnummer mit einem W.-Profil verknüpft ist. Wenn eine Übereinstimmung festgestellt wird, kann das entsprechende Nutzerprofil, welches weitere Daten bereithält, angezeigt werden. Im Grundsatz sollte mit dieser Anwendung das Auffinden von Freunden und Bekannten auf W. erleichtert werden.

Daneben ist die Beklagte Anbieterin des W.-Messenger-Dienstes (der „Messenger-Dienst“). Bei der Anwendung handelt es sich um eine integrierte Chat-Funktion, auf die auch über eine separate App zugegriffen werden kann und die es W.-Nutzern ermöglicht, auf verschiedene Weise, u.a. über Text-und/oder Audionachrichten, direkt mit anderen Nutzern und Unternehmen zu kommunizieren. Die Kommunikation erfolgt sicher über Plattformen und Geräte hinweg. Es besteht keine Verpflichtung zur Nutzung des Messenger-Dienstes bei der Nutzung von W.. 15

Der Kläger ist Inhaber eines W.-Accounts und nutzt die von der Beklagten betriebene Plattform. Er ist mit seinem vollständigen Namen sichtbar und meldete sich mit der E-Mail-Adresse H.@Q..org an. Auch er gab im Rahmen des Registrierungsprozesses seine Mobilfunknummer an. Nach der Zielgruppenauswahl war die Handynummer auf dem Profil des Klägers nicht zu sehen. Nach den Suchbarkeitseinstellungen war die Suche nach dem klägerischen Profil mittels dessen Mobilfunknummer jedoch aktiviert und wie vorgegeben in dem gesamten relevanten Zeitraum auf ‘‘alle (everyone)‘‘ eingestellt. 16

Zwischen Januar 2018 und September 2019 kam es dazu, dass Dritte in großem Umfang Daten von E.-nutzern mittels sog. Web-Scrapings abschöpften. Dabei handelt es sich um ein automatisiertes Verfahren zur Sammlung und Speicherung von öffentlich zugänglichen Daten. 17

Wenngleich die exakte Vorgehensweise unbekannt geblieben ist, geht die Beklagte davon aus, dass diese Dritten dazu die Kontakt-Import-Funktion (CIT) nutzten, indem sie eine Vielzahl von zufällig bzw. systematisch erzeugten Zahlenkombinationen in ein virtuelles Adressbuch eingaben und dieses mit W. synchronisierten. Kam es dabei zufällig zu einer Übereinstimmung mit einer tatsächlich hinterlegten Rufnummer, wurde ihnen das zu dieser Nummer gehörige Profil angezeigt. 18

Über einen Besuch des so angezeigten Profils gelangten die Unbekannten dann zum einen an die „immer öffentlich“ eingestellten Daten, namentlich den Namen, das Geschlecht und die W.-ID der jeweiligen Nutzer. Zugänglich waren den Unbekannten darüber hinaus die aufgrund der Privatsphäreeinstellungen der Nutzer öffentlich einsehbaren Daten. 19

Anfang April 2021 wurden diese Daten von über 500 Millionen Nutzern aus 106 Ländern, die in dem oben genannten Zeitraum im Wege des sog. „Scrapings“ erlangt wurden, von Unbekannten im Internet veröffentlicht und verbreitet. 20

Dass auch Daten des Klägers von diesem Vorfall betroffen waren, ist unstreitig. 21

Die Beklagte informierte die zuständige Datenschutzbehörde - die R. - nicht über den Vorfall; auch wurde der Kläger wegen der Entwendung und Veröffentlichung seiner Daten nicht unmittelbar von der Beklagten informiert. 22

Daneben erhält die Beklagte Informationen über Aktivitäten der Nutzer außerhalb der T.-Technologien, wenn sich Drittanbieter dafür entscheiden, die Technologien der Beklagten auf 23

ihren Websites oder Anwendungen zu verwenden und/oder zu installieren, um der Beklagten Informationen über ihre Besucher zu senden.

Die Drittanbieter sind rechtlich verpflichtet, vor Verwendung solcher Technologien diesbezüglich klare und umfassende Informationen zur Verfügung zu stellen und (wenn erforderlich) die Einwilligung der Besucher der Website einzuholen. Schließlich ist jeder Drittanbieter dafür verantwortlich, zu gewährleisten, dass die Erfassung und Übermittlung von Daten an die Beklagte auf einer gültigen Rechtsgrundlage beruht. Diese zweit- und drittgenannte Verpflichtung erfordern üblicherweise, dass der Besucher einer Website seine Einwilligung über ein Cookie-Banner beim ersten Aufruf jeder Website erteilt. 24

Zusätzlich zu der rechtlichen Verpflichtung der Drittanbieter, die Einwilligung des Nutzers zu Cookies auf der Website oder Anwendung der Drittanbieter einzuholen, zeigt die Beklagte ihren registrierten Nutzern proaktiv einen Cookie-Banner an. Die Beklagte verwendet Daten, die sie von ihren Cookies und ähnlichen Technologien von Websites und Anwendungen Dritter erhält, nur, nachdem der Nutzer dieser Verwendung über das Cookie-Banner zugestimmt hat. 25

Die Verwendung der Daten kann danach jederzeit über die individuellen Kontoeinstellungen angepasst werden 26

Auch der Kläger kann die entsprechenden Einstellungen jederzeit entsprechend abändern. Sowohl in der Datenschutzrichtlinie als auch im Hilfebereich und in den Cookie-Einstellungen gibt es jeweils Anleitungen und Hilfestellungen, um die Einstellungen über die T.-Technologien hinweg zu individualisieren. Unter Eingabe der hier in Frage kommenden Schlagwörter, wie etwa „Aktivitäten außerhalb der T.-Technologien“ oder „Off-W.-Daten“, führt bereits eine einfache Desktoprecherche zu den relevanten Einstellungsseiten der Beklagten. 27

Der Hilfebereich sieht auch eine Anleitung dahingehend vor, wie Nutzer die Verknüpfung ihrer Aktivitäten außerhalb der T.-Technologien von ihrem Konto trennen und die Verknüpfung mit künftigen Aktivitäten aufheben können. 28

Die Beklagte übermittelt Daten unter anderem auch der europäischen Nutzer an die N.. 29

Der W.-Dienst ist ein globaler Online-Kommunikationsdienst und Dienst für das Teilen von Online-Inhalten, dessen eigentlicher Zweck es ist, Nutzern die Möglichkeit zu geben, mit anderen Nutzern auf der ganzen Welt auf vielfältige Weise in Kontakt zu treten und Inhalte zu teilen. Der W.-Dienst ist daher zwangsläufig auf den freien Fluss personenbezogener Daten zwischen der EU / dem EWR und den USA angewiesen. In tatsächlicher Hinsicht sind Datenübermittlungen notwendig, damit die Beklagte den W.-Dienst Hunderten von Millionen Nutzern in der EU / dem EWR (die „MPIL-Nutzer“) bereitstellen und ihren vertraglichen Verpflichtungen zur Bereitstellung des W.-Dienstes entsprechend den Nutzungsbedingungen nachkommen kann. 30

Dementsprechend wäre es der Beklagten ohne die Datenübermittlungen nicht möglich, MPIL-Nutzern den W.-Dienst bereitzustellen. Ohne solche Datenübermittlungen in die USA müsste die Beklagte die Bereitstellung des W.-Dienstes für MPIL-Nutzer gänzlich einstellen. 31

Im Anwendungsbereich von X. ist die US-Regierung mit Blick auf die Interessen der nationalen Sicherheit dazu befugt, gezielte Überwachungen durchzuführen, um die USA und ihre Verbündeten vor feindlichen ausländischen Gegnern, einschließlich Terroristen, Spionen 32

und Bedrohungen der Cybersicherheit, zu schützen. Allgemein ermächtigt Z. US-Regierungsbehörden dazu, Anbieter elektronischer Kommunikationsdienste, wie MPI, zur Herausgabe von Aufzeichnungen zu zwingen, die sich in „ihrem Besitz, ihrer Verwahrung oder unter ihrer Kontrolle“ befinden. Dazu können auch Aufzeichnungen im Zusammenhang mit MPIL-Nutzern gehören. Das Recht der USA verbietet es Anbietern elektronischer Kommunikationsdienste, Informationen zu erhaltenen Anfragen nach Z. Dritten gegenüber offenzulegen. Es ist MPI also gesetzlich untersagt, sich zu Anfragen zu äußern, die sie möglicherweise nach Z. zu MPIL-Nutzerdaten erhält.

Die Beklagte veröffentlicht unter anderem in ihren Transparenzberichten Informationen über die Möglichkeit, dass Daten der Nutzer der Beklagten Gegenstand von Anfragen der US-Strafverfolgungs- und Geheimdienstbehörden sein können. Enthalten sind dort Statistiken darüber, wie viele V.-Anfragen jedes Jahr eingehen. Weitere Informationen stehen den Nutzern, einschließlich der Klagepartei, im M. Center zur Verfügung. 33

Mit anwaltlichem Anspruchsschreiben vom 25.07.2023 stellte der Kläger bei der Beklagten eine Anfrage nach Art. 15 P. und forderte sie zugleich auf, einen immateriellen Schadenersatz wegen des bekannten Datenlecks an sie zu leisten und machte Auskunfts- und Unterlassungsansprüche geltend. 34

Mit Schreiben vom 20.09.2023 teilte die Beklagte dem Kläger Folgendes mit: 35

„T. A. hält keine Kopie der Rohdaten, welche die durch Scraping abgerufenen Daten enthalten. Auf Grundlage der bislang vorgenommenen Analysen ist es T. A. jedoch gelungen, der Nutzer ID Ihres Mandanten die folgenden Datenkategorien zuzuordnen, die nach unserem Verständnis in den durch Scraping abgerufenen Daten erscheinen und mit den auf dem W.-Profil Ihres Mandanten verfügbaren Informationen übereinstimmen (die „Datenpunkte“): 36

- *Nutzer ID* 37
- *Vorname*
- *Nachname*
- *Land*
- *Geschlecht […]“*

Wegen des weiteren Inhalts wird auf das Schreiben der Beklagten verwiesen (Bl. 744 d.A.). 38

Mit weiterem anwaltlichem Schreiben vom 13.12.2023 forderte der Kläger die Beklagte zur Vornahme der geforderten Handlungen und Erklärungen betreffend den „Messenger“-Dienst, die Weitergabe der Daten in die USA sowie das Sammeln von „Off-W.“-Daten innerhalb einer Frist von 2 Wochen ab dem 13.12.2023 auf. 39

Auf dieses Schreiben antwortete die Beklagte ihrerseits mit außerprozessualem Schreiben vom 08.01.2024. Insbesondere erklärte die Beklagte dem Kläger darin, wie er auf seine W.-Daten zugreifen kann und wies ihn auf die maßgeblichen Abschnitte der Datenschutzrichtlinie und das verfügbare Selbstbedienungs-Tool („Zugriff auf deine Informationen“ und „Deine Informationen herunterladen“) hin, dass es W.-Nutzern ermöglicht, ihre W.-Daten aufzurufen und zu verwalten. 40

Der Kläger behauptet, die Beklagte hätte in Bezug auf die Verwendung des Kontakt-Import-Tools u.a. eine Begrenzung für die Höchstzahl der Eingaben von Telefonnummern durch eine 41

Person in der Kontakt-Import-Funktion festlegen können. Die Beklagte sei bereits im Jahr 2017 durch den belgischen IT-Sicherheitsexperten S. darüber informiert worden, dass das in Rede stehende Kontakt-Import-Tool in Bezug auf unbefugte Verwendung verwundbar sei.

Zudem seien die Daten beispielsweise auf der Internetseite K..com veröffentlicht worden. Bei diesem Forum handele es sich um ein „ Hacker"-Forum, welches damit in Verbindung gebracht werde, dass illegal abgeschöpfte Daten — wie gegenständlich — hinterlegt und ausgetauscht werden, um diese unter anderem für kriminelle Vorgehen zu nutzen, beispielsweise Computerbetrug oder gezielte Phishing-Attacken. 42

Der Kläger meint, das Scraping bei der Beklagten sei erst durch eine Lücke im Kontakt-Import Tool ermöglicht worden. Dies hätten die Angreifer durch die Nutzung eines sog. „O." erreichen können. Dabei handele es sich um eine Software, welche L.-Geräte, mithin gängige Smartphones, auf einem PC simulieren könne. Dem entsprechend könnten auch die Anwendungen eines Smartphones simuliert werden, daher auch ein Adressbuch. 43

In ein solch simuliertes Adressbuch könnten in der Folge beispielsweise mehrere zehntausend, gegebenenfalls auch generisch erzeugte, Telefonnummern eingepflegt werden, um in der Folge dieses Adressbuch auf W. hochzuladen. Sofern eine Übereinstimmung mit einer bei W. hinterlegten Telefonnummer festgestellt werde, könnte so das entsprechende Nutzer-Profil angezeigt werden. 44

Der Kläger behauptet weiter, der Prozess und die Einstellungen zur Datensicherheit für die Nutzer von W. seien insgesamt geprägt durch datenschutzunfreundliche Einstellungen sowie einer Vielzahl von schwer verständlichen Informationen und unklarer Angaben. 45

Dies sei bereits bei der Erstellung eines W.-Accounts zu konstatieren. 46

Bei der Erstellung eines Profils werde der angehende Nutzer mit einer Informationsflut konfrontiert, die sich aus Nutzungsbedingungen, der Verwendung von Cookies sowie den Datenschutzrichtlinien zusammensetze. Jeder dieser Teilaspekte könne über eine kleine Verlinkung im unteren Teil der Anmeldemaske erreicht werden. Es sei bereits unklar, weswegen zwischen Datenschutzrichtlinien und der Verwendung von Cookies differenziert werde, obwohl die Cookie-Verwendung evident ein dem Datenschutz innewohnendes Thema sei. 47

Durch die zum Teil anhand der Benennung inhaltlich nicht ohne Weiteres zu unterscheidenden Optionen und der Vielzahl an weiteren Einstellungsmöglichkeiten sei mit hoher Wahrscheinlichkeit zu erwarten, dass ein Nutzer die voreingestellten Standardeinstellungen beibehalte und nicht selbstständig ändere, insbesondere unter Berücksichtigung des kollektiven Bewusstseins, dass im Internet grundsätzlich ein hohes Datenschutzniveau sichergestellt sein müsse. Aus diesem Grund komme den Voreinstellungen der Beklagten eine erhöhte Bedeutung zu. 48

Die Beklagte habe auch an keiner Stelle erklärt, dass die Telefonnummern, welche von den Nutzern ausschließlich zur Nutzung im Rahmen der Authentifizierung verwendet werden sollten, im Weiteren für andere Zwecke im Netzwerk genutzt werden sollten, wie beispielsweise im Rahmen der Anwendung des Kontakt-Import-Tools. Diese (missbräuchliche) Nutzung sei von der Beklagten nicht offengelegt worden, sodass die Nutzer auch nicht gewusst hätten, dass ihre ausschließlich zu Sicherheitszwecken übergebene Telefonnummer auch für andere Zwecke genutzt werde. 49

50

Die Beklagte habe es von Anfang an darauf angelegt, die wahren Hintergründe des gegenständlichen Datenlecks zu verschleiern und herunterzuspielen. Daher sei seitens der Beklagten auch keine ausreichende Information betreffend die Datenabschöpfung erfolgt.

Durch den Datenschutzverstoß der Beklagten seien bereits kriminelle Vorgehen in Bezug auf die abgeschöpften Daten in Gang gesetzt worden. Konkret handele es sich um das sogenannte „Smishing". Dies beschreibe eine Angriffsmethode, die zum Diebstahl von Zugangsdaten über gefälschte Nachrichten oder E-Mails führen solle. Konkret seien den von dem Datenleck Betroffenen SMS-Nachrichten durch einen ihnen unbekannten Kontakt übersendet worden. Der in der Nachricht enthaltene Link habe nach einem Klick zum Download der mit dem Link verknüpften Schadsoftware geführt. Die Nachricht sei als Benachrichtigung über die Versendungsbestätigung eines Pakets getarnt worden. 51

Die einzige Möglichkeit, den Erhalt von Spam-Nachrichten zu unterbinden, sei, die eigene Nummer auszutauschen. Dies sei jedoch mit hohem organisatorischem und auch finanziellem Aufwand verbunden, insbesondere der Wechsel der Telefonnummer beim jeweiligen Provider. 52

Darüber hinaus seien die veröffentlichten Daten des Klägers keineswegs mehr sicher und die Gefahr einer unbefugten und schädigenden Verwendung müsse stets in Betracht gezogen werden. 53

Dem entsprechend habe der Kläger durch das mangelhafte und pflichtwidrige Verhalten der Beklagten die Kontrolle über seine Daten vollständig verloren, da er nicht mehr bestimmen könne, wer welche Daten wann zur Kenntnis und Verarbeitung erhalte. Er sei der Gefahr des Zugriffs einer Vielzahl von Personen auf die Daten ausgesetzt, welchen er in keiner Weise mehr beeinflussen könne, dies insbesondere unter Berücksichtigung des Umstands, dass er auch nicht über das Datenleck informiert worden sei. Jeder Betroffene müsse daher fortlaufend darüber besorgt sein, dass seine personenbezogenen Daten in vielfacher Art und Weise gegen seinen Willen und mit einem hohen Risiko für seine persönliche wie auch finanzielle Lage missbraucht werden könnten bzw. auch bereits missbraucht worden seien. 54

Konkret sei der Kläger nach dem Datenleck von vielen ungebetenen und unerwünschten E-Mail-Nachrichten sowie SMS Nachrichten betroffen gewesen und habe sich hierüber sehr geärgert. Dieser Ärger halte auch bis zum heutigen Tag an, was sich insbesondere an dem eingetretenen Kontrollverlust der klägerischen Daten festmache. 55

Der Kläger ist der Ansicht, die Beklagte habe verschiedene Datenschutzverstöße begangen. 56

So habe sie es unter andere, entgegen Art 24 Abs. 1 P. unterlassen, geeignete technisch-organisatorische Maßnahmen zu errichten, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt ist. 57

Da die Beklagte weder die Aufsichtsbehörde noch die betroffenen Nutzer unverzüglich benachrichtigt habe, habe sie gegen Art. 34 und Art 33 P. verstoßen. 58

Hinsichtlich des von der Beklagten bereitgestellten Messenger-Dienstes behauptet der Kläger, dieser werde durch die Beklagte systematisch und automatisiert überwacht. Dies geschehe im Rahmen der Datenschutzrichtlinie von W., wonach W. 59

auch die Erfassung der „Aktivität auf allen (..) Produkten“ für notwendig erachte. Eine Einschränkung dieser Analyse- und Erfassungstätigkeit findet sich in der 60

Datenschutzrichtlinie nicht.

Es müsse also davon ausgegangen werden, dass das „crawling“ der Inhalte das Standardprocedere sei, von welchem nicht abgewichen werde und welches auch nicht deaktiviert werden könne. Der Kläger ist der Ansicht, das Durchsuchen und Lesen seiner privaten Nachrichten verstoße gegen Art 5 und 10 GG. Dies rufe mehr als ein bloßes Unwohlsein hervor. Bei dem Kläger seien erhebliche Ängste entstanden. Er fühle sich sowohl in der Meinungsäußerung der Postings als auch bei den privaten Nachrichten (Messenger) nicht mehr frei. 61

Zudem sammle die Beklagte massenhaft „Off-W.-Daten“, ohne dass eine Einwilligung durch die Nutzer dafür eingefordert werde. 62

Ferner habe die Beklagte sämtliche personenbezogene Daten des Klägers, die aus dem klägerischen W.-Account ersichtlich seien und mit diesem verbunden seien, in die USA und auch an dortige Geheimdienste, insbesondere der F. (I.), weitergeleitet zur anlasslosen Überprüfung und Untersuchung. 63

Der Kläger ist aber der Ansicht, eine Übermittlung von Daten in sogenannte Drittländer, zu denen die USA gehöre, sei nur dann zulässig, wenn das schützende Niveau der P. in dem Land, in das die Daten übermittelt werden, ebenfalls gewährleistet werde. 64

Folgende personenbezogene Daten würden unter anderem von der Beklagten in die USA übermittelt: 65

? Kommunikation zwischen Benutzern (Messenger = private Nachrichten) und zugehörige Informationen über die Nutzung der Produkte und Dienstleistungen 66

? alle Informationen, der Kläger im W.-Profil schreibt, teilt und hochlädt und über Personen, die das eigene J. profil besuchen, darauf zugreifen oder auf andere Weise mit den Produkten und Diensten von W. interagieren 67

? Informationen bei der Nutzung der von W. angebotenen Dienste bei denen die Benutzer Informationen bereitstellen wie z.B. Profilinformationen, gepostete Fotos und Videos oder wenn diese geteilt werden 68

? Informationen in Bezug auf den jeweiligen Nutzer, die andere Nutzer bereitstellen oder hochladen der bereitgestellten z.B. importierte Kontakte oder Foto von anderen Benutzern 69

Derartige Daten könnten zur politischen Manipulation verwendet werden. 70

Der Anspruch auf Schadenersatz wegen Nichterteilung einer Auskunft, ergebe sich unmittelbar aus Art. 15 Abs. 1 iVm 82 Abs. 1 P., wobei ein Betrag von mindestens 2.000 € angemessen sei. 71

Der Anspruch auf Unterlassung ergebe sich entweder aus Art. 17 P. oder § 1004 Abs. 1 Satz 2 BGB analog, § 823 Abs. 2 BGB iVm. Art. 6 Abs. 1 P.. 72

Der Kläger habe schließlich einen Anspruch gegen die Beklagte auf Auskunft über die personenbezogenen Daten, welche von der Beklagten verarbeitet wurden, Art. 15 Abs. 1 P.. 73

Der Kläger beantragt: 74

75

1. Die Beklagte wird verurteilt, an die Klagepartei immateriellen Schadensersatz als Ausgleich für Datenschutzverstöße und die Ermöglichung der unbefugten Ermittlung der Telefonnummer sowie weiterer personenbezogener Daten der Klägerseite zu zahlen, dessen Höhe in das Ermessen des Gerichts gestellt wird, jedoch mindestens 3.000,00 EUR betragen muss, nebst Zinsen in Höhe von fünf Prozentpunkten über dem jeweiligen Basiszinssatz seit dem 05.08.2023.

2. Die Beklagte wird weiter verurteilt, an die Klagepartei immateriellen Schadensersatz als Ausgleich für Datenschutzverstöße hinsichtlich der anlasslosen Überwachung von im Wege des W.-Messenger-Dienstes versandten und erhaltenen Chat-Nachrichten der Klagepartei sowie der Sammlung, Nutzung und Auswertung der „Off-W.-Daten“ der Klagepartei an die Klägerseite zu zahlen, dessen Höhe in das Ermessen des Gerichts gestellt wird, jedoch mindestens 2.000,00 EUR betragen muss, nebst Zinsen in Höhe von fünf Prozentpunkten über dem jeweiligen Basiszinssatz seit Rechtshängigkeit. 76

3. Die Beklagte wird weiter verurteilt, an die Klagepartei immateriellen Schadensersatz als Ausgleich für Datenschutzverstöße hinsichtlich der Weitergabe und Übermittlung personenbezogener Daten der Klägerseite in die USA, insbesondere an die dortige C. (I.) zu zahlen, dessen Höhe in das Ermessen des Gerichts gestellt wird, jedoch mindestens 2.000,00 EUR betragen muss, nebst Zinsen in Höhe von fünf Prozentpunkten über dem jeweiligen Basiszinssatz seit Rechtshängigkeit. 77

4. Es wird festgestellt, dass die Beklagte verpflichtet ist, der Klagepartei alle zukünftigen Schäden zu ersetzen, die der Klagepartei 78

a) durch den unbefugten Zugriff Dritter auf das Datenarchiv der Beklagten, der nach Aussagen der Beklagten im Jahr 2019 erfolgte und 79

b) durch die anlasslose Überwachung von im Wege des W.-Messenger-Dienstes versandten und erhaltenen Chat-Nachrichten der Klagepartei sowie der Sammlung, Nutzung und Auswertung der „Off-W.-Daten“ sowie 80

c) durch die Weitergabe und Übermittlung personenbezogener Daten der Klägerseite in die USA, insbesondere an die dortige C. (I.) 81

entstanden sind und / oder noch entstehen werden. 82

5. Die Beklagte wird verurteilt, an die Klägerseite für die Nichterteilung einer den gesetzlichen Anforderungen entsprechenden außergerichtlichen Datenauskunft im Sinne des Art. 15 DS-GVO einen weiteren immateriellen Schadensersatz, dessen Höhe in das Ermessen des Gerichts gestellt wird, den Betrag von 2.000,00 € aber nicht unterschreiten sollte, nebst Zinsen in Höhe von 5%-Punkten über dem Basiszinssatz seit dem 05.08.2023 zu bezahlen. 83

6. 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, 84

zu unterlassen, 85

86

a.) personenbezogene Daten der Klagepartei, namentlich Telefonnummer, W.-ID, Familienname, Vorname, 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 Klagepartei auf Grundlage einer Einwilligung zu verarbeiten, die wegen der unübersichtlichen und unvollständigen Informationen durch die Beklagte erlangt wurde, namentlich ohne eindeutige Information darüber, dass die Telefonnummer auch bei Einstellung auf „privat“ noch durch Verwendung des Kontakt-Import-Tools verwendet werden kann, wenn nicht explizit hierfür die Berechtigung verweigert und, im Falle der Nutzung der W.-Messenger-App, hier ebenfalls die Berechtigung verweigert wird. 87

7. Die Beklagte wird weiter 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, 88

a) Chat-Nachrichten der Klagepartei, welche mittels des „W.-Messenger“-Dienstes versandt werden und wurden, anlasslos zu überwachen, 89

b) „Off-W.-Daten“ der Klagepartei zu sammeln, nutzen und auszuwerten, 90

c) personenbezogene Daten der Klagepartei in die USA, insbesondere die F. (I.) zu übermitteln. 91

8. Die Beklagte wird verurteilt, der Klagepartei Auskunft 92

a) über die Klagepartei 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 Kontakt-Import-Tools erlangt werden konnten, 93

b) über die überwachten, ausgewerteten und gespeicherten Daten aus der Überwachung des W.-Messengers zu erteilen, namentlich Chat-Protokolle vorzulegen und deren interne Bewertung offenzulegen, sowie diese, sofern anlasslos gespeichert, zu löschen, 94

c) zu erteilen, welche „Off-W.-Daten“ durch die Beklagte an der IP-Adresse der Klägerseite gesammelt wurden und zu welchem Zweck diese gespeichert und verwendet wurden, sowie diese, sofern anlasslos gespeichert, zu löschen, 95

d) zu erteilen, in welcher konkreten Hinsicht die Klägerseite von der Übermittlung der personenbezogenen Daten der Klägerseite in die USA, insbesondere an die dortige F. (I.) betroffen war, also wer wann auf welche Daten der Klägerseite zugegriffen hat und welche genauen personenbezogenen Daten der Klägerseite von wem eingesehen wurden. 96

9. Die Beklagte wird verurteilt, die Klagepartei von vorgerichtlichen Rechtsanwaltskosten in Höhe von 1.019,83 EUR gegenüber der Fachanwaltskanzlei Seehofer freizustellen. 97

98

Die Beklagte beantragt,

die Klage abzuweisen. 99

Die Beklagte ist der Ansicht, die Klage sei teilweise schon unzulässig, jedenfalls aber unbegründet. 100

Die Beklagte behauptet, die Suchbarkeits-Einstellungen seien klar und leicht zu finden gewesen. 101

Es liege kein Datenschutzverstoß vor. Es seien nur solche Daten des Klägers „gescrapt“ worden, die ohnehin öffentlich zugänglich gewesen seien, weil der Kläger diese – insoweit unstreitig –in den Privatsphäreeinstellungen als öffentlich einsehbar eingestellt habe. 102

Die Daten seien weder durch Hacking noch infolge eines Fehlers oder Sicherheitsverstoßes in ihrem System, sondern durch das automatisierte, massenhafte Sammeln von ohnehin öffentlich einsehbaren und damit nicht vertraulichen Daten erlangt und an anderer Stelle zugänglich gemacht worden. 103

Der Kläger hätte von Anfang an oder zu jeder Zeit ihre Privatsphäre-Einstellungen hinsichtlich der Daten wie Telefonnummer, Wohnort, Stadt, Beziehungsstatus, Geburtstag und E-Mail-Adresse individualisieren und so die Einsehbarkeit begrenzen können. 104

Die Standard-Voreinstellungen würden sich an dem Zweck der Plattform, mit anderen Personen in Kontakt zu treten, orientieren. 105

Die "Scraper" hätten dementsprechend lediglich die diesem Zweck dienenden Funktionen ausgenutzt. Es sei daher grundsätzlich unmöglich, Scraping öffentlich einsehbarer Daten völlig zu verhindern, ohne den Zweck der Plattform durch Beseitigung der Funktionen zu unterlaufen. Das Mögliche sei jedoch zur Verhinderung getan worden bzw. werde getan. 106

Insoweit seien die Suchbarkeitseinstellung für die Nutzer auch nicht von schwer verständlichen Informationen und unklaren Angaben geprägt. 107

Die Beklagte stelle allen Nutzern inklusive des Klägers alle in Art. 13 und Art. 14 P. festgelegten Informationen zur Datenverarbeitung zur Verfügung. Es habe zudem eine umfassende und transparente Information über die Möglichkeit der Anpassung ihrer Suchbarkeitseinstellungen und Zielgruppenauswahl gegeben, woraus sich nachvollziehbar ergebe, wer bestimmte persönliche Informationen, die der Nutzer in seinem W.-Profil hinterlegt habe, einsehen könne. Diese Einstellungen habe der Kläger jederzeit anpassen können. 108

Insgesamt habe die Beklagte alle ausreichenden Sicherheitsvorkehrungen vorgenommen, um ein Ausnutzen des bereitgestellten Tools zu verhindern, es bestehe also keine Sicherheitslücke. Sie habe nicht gegen Art. 24, 32 P. verstoßen, sondern vielmehr angemessene technische und organisatorische Maßnahmen ergriffen, das Risiko von Scraping zu unterbinden. So habe sie u.a. Übertragungsbeschränkungen implementiert, die die Anzahl von Anfragen bestimmter Daten reduzierten, welche pro Nutzer oder von einer bestimmten IP-Adresse in einem bestimmten Zeitraum gemacht werden könnten. Weiterhin habe sie eine Bot-Erkennung eingesetzt, zudem habe sie U.-Abfragen genutzt. 109

Die Beklagte bestreitet mit Nichtwissen, dass der Kläger infolge des Scraping-Sachverhalts unregelmäßig Kontaktversuche, etwa via SMS und E-Mail, mit offensichtlichen 110

Betrugsversuchen und potenziellen Virenlinks erhalte.

Die Beklagte meint, die von dem Kläger geltend gemachten Verstöße gegen Art. 13, 14, 15, 24, 25, 32, 34 P. seien bereits nicht vom Anwendungsbereich des Art. 82 P. erfasst. Das klägerische Auskunftsersuchen habe sie ordnungsgemäß beantwortet. 111

Entgegen dem spekulativen klägerischen Vorbringen wahre die Beklagte sehr wohl die Vertraulichkeit der privaten Kommunikation zwischen Nutzern, die sich über den Messenger-Dienst austauschen. Die durch die Beklagte vorgenommene Datenverarbeitung (auch im Zusammenhang mit dem Messenger-Dienst) erfolge stets gestützt auf eine Rechtsgrundlage und sei mithin rechtmäßig. Gemäß Art. 3 der CSAM-Verordnung setze die Beklagte Medienabgleichstechnologien ein, die bei der Aufdeckung, Entfernung und Meldung des Austauschs von Medien, die die Ausbeutung von Kindern zeigen, helfen. Diese Medienabgleichstechnologien würden eine eindeutige digitale Signatur eines Bildes (eine unter dem Namen „Hash“ bekannte Zahlenreihe oder -folge) erstellen, die dann mit einer Datenbank, die Signaturen (Hashes) zuvor identifizierter (d.h. bekannter und bestätigter) kinderpornografischer Inhalte enthält, abgeglichen werde („CSAM-Scanning“). Dies sei keine anlasslose, systematische und automatisierte Überwachung durch die Beklagte, sondern erlaube es der Beklagten vielmehr rechtmäßig, Schutz, Integrität und Sicherheit bei T.-Produkten zu fördern. 112

Der Vortrag des Klägers zur Verarbeitung von Daten außerhalb der Plattform sog. „Off-W.-Daten“ sei schon unschlüssig und unsubstantiiert. Der Kläger trage insoweit nicht vor, in welcher Hinsicht die Verarbeitung beanstandet werde. 113

Die Beklagte hat mit Schriftsatz vom 20.03.2024 die Einrede der Verjährung erhoben. 114

Wegen der weiteren Einzelheiten des Sach- und Streitstandes wird auf die gewechselten Schriftsätze nebst Anlagen verwiesen. 115

Entscheidungsgründe 116

Die Klage hat in der Sache keinen Erfolg. 117

Sie ist bezüglich der Anträge 4), 6a), 6b), 7a), 7b), 8b) und 8c) bereits unzulässig, im Übrigen unbegründet. 118

I. 119

1. 120

Bedenken gegen die Zulässigkeit der Klageanträge 1), 2), 3), 5), 7c), 8a) und d) bestehen nicht. 121

Die Anwendbarkeit deutschen Rechts folgt aus den Art. 6 Abs. 1 und Art. 18 Abs. 1 2. Alt EuGVVO (Brüssel Ia-VO). Gemäß Art. 1 Abs. 1 EuGVVO ist die EuGVVO sachlich anwendbar auf Zivil- und Handelssachen. Vorliegend handelt es sich um eine Zivilsache. 122

Ein ausschließlicher Gerichtsstand gemäß Art. 24 EuGVVO ist hier nicht ersichtlich. Gemäß Art. 18 Abs. 1 2. Alt EuGVVO kann die Klage eines Verbrauchers gegen den anderen Vertragspartner entweder vor den Gerichten des Mitgliedstaats erhoben werden, in dessen Hoheitsgebiet dieser Vertragspartner seinen Wohnsitz hat, oder ohne Rücksicht auf den Wohnsitz des anderen Vertragspartners vor dem Gericht des Ortes, an dem der Verbraucher 123

seinen Wohnsitz hat. Letzteres ist im Hinblick auf den Wohnsitz des Klägers der Fall.

Die sachliche Zuständigkeit folgt aus §§ 23 Nr. 1, 71 Abs. 1 GVG, da der Streitwert entsprechend der erfolgten Festsetzung mehr als 5.000,00 EUR beträgt. 124

Die örtliche Zuständigkeit folgt jedenfalls aus dem besonderen Gerichtsstand des Art. 79 Abs. 2 Satz 2 P., § 44 Abs. 1 Satz 2 BDSG im Hinblick auf den Wohnsitz des Klägers im hiesigen Gerichtsbezirk. 125

2. 126

Der Klageantrag zu 4.) ist dagegen mangels Feststellungsinteresses unzulässig. 127

Danach hat das Gericht berücksichtigt, dass bei anderen als reinen Vermögensschäden bereits die Möglichkeit materieller oder weiterer immaterieller Schäden für die Annahme eines Feststellungsinteresses i.S.d. § 256 ZPO ausreicht. 128

Ein Feststellungsinteresse ist danach nur zu verneinen, wenn aus der Sicht des Geschädigten bei verständiger Würdigung kein Grund besteht, mit dem Eintritt eines derartigen Schadens wenigstens zu rechnen (OLG Hamm, Urteil vom 15.08.2023 – 7 U 19/23). 129

So liegt es hier. 130

Dem Kläger ist infolge des Datenlecks bisher kein materieller Schaden entstanden. Warum nunmehr Jahre später noch mit dem Eintritt eines materiellen Schadens zu rechnen sein soll, ist nicht ersichtlich. Ein solcher Schaden ist rein theoretischer Natur und vermag kein Feststellungsinteresse zu begründen. 131

Dasselbe gilt für behauptete immaterielle Schäden. Insoweit wird auf die nachfolgenden Ausführungen zu dem Schadensersatzanspruch des Klägers verwiesen. 132

Gleiches gilt hinsichtlich der Feststellung zukünftigen Schadensersatzes betreffend die behauptete Überwachung des W.-Messenger-Dienstes sowie die Verarbeitung von „Off-W.-Daten“ und die Weitergabe von Daten in die USA. 133

3. 134

Die Klageanträge zu 6 a und b) sind ebenfalls unzulässig. 135

Zunächst enthalten die Anträge mit der geforderten Androhung nach § 890 Abs. 2 ZPO ein unzulässiges Antragsbegehren. Denn der Kläger fordert in der Hauptsache ein aktives Tun, das als vertretbare Handlung gem. § 887 ZPO zu vollstrecken wäre. Denn sein Begehren erstreckt sich darauf, dass die Beklagte zukünftig Kontaktimportfunktionen nur im Einklang mit den einzuhaltenden Sicherheitsvorkehrungen freischaltet, um Zugriffe unbefugter Dritter nach Möglichkeit zu verhindern (vgl. OLG Hamm, Urteil vom 15.08.2023 – 7 U 19/23). 136

Darüber hinaus genügen die Anträge nicht den Anforderungen des § 259 ZPO, wonach Klage auf künftige Leistung erhoben werden kann, wenn die Besorgnis gerechtfertigt ist, dass der Schuldner sich der rechtzeitigen Leistung entziehen werde. 137

Derartige Umstände liegen nicht vor. 138

139

Zunächst hat die Beklagte die Such- und Kontaktimportfunktion hinsichtlich der Mobilfunknummer abgestellt.

Soweit danach die Klage auf zukünftige Leistung der Beklagten auf den Fall gerichtet ist, dass andere Personen Wege finden, die neuen Funktionen zu umgehen, besteht keine Besorgnis, dass die Beklagte ihre Leistung rechtzeitig erbringt. 140

Denn die Beklagte hat nach Bekanntwerden des Vorfalls die streitgegenständliche Funktion beseitigt und sodann weitere Maßnahmen zur Verhinderung getroffen. Sie hat ein hohes Eigeninteresse daran, dass sich ein solcher Vorfall nicht wiederholt. 141

Eine solche Leistungsklage ist ohnehin nicht erhoben, so dass dahinstehen kann, ob hierauf überhaupt ein Leistungsanspruch bestünde. 142

4. 143

Auch die Klageanträge zu 7a) und 7b) sind bereits unzulässig. 144

a. 145

Soweit der Kläger begehrt, die Beklagte zu verurteilen, es bei Meidung eines Ordnungsgeldes zu unterlassen, die Chat-Nachrichten des Klägers, welche mittels des „W.-Messenger“-Dienstes versandt werden, anlasslos zu überwachen, ist der Antrag schon nicht bestimmt im Sinne des § 253 Abs. 2 Nr. 2 ZPO. Das Wort „anlasslos" schränkt das Unterlassungsbegehren in objektiv nicht abgrenzbarer Weise ein. Ein entsprechender Ausspruch wäre nicht vollstreckungsfähig (vgl. dazu Urteil des Landgerichts Passau vom 16.02.2024 – 1 O 616/23). 146

b. 147

Dem Unterlassungsantrag des Klägers betreffend das Sammeln, Nutzen und Auswerten sog. „Off-W.“-Dateien fehlt bereits das Rechtschutzbedürfnis. Denn insoweit kann der Kläger nach dem unbestrittenen Vortrag der Beklagten dies selbst über die Einstellungen steuern. Die Beklagte hat dem Kläger die genaue Vorgehensweise mit Schreiben vom 08.01.2024 erläutert. Da ihm ein einfacherer Weg zur Erreichung ihres Rechtsschutzziels zur Verfügung steht, fehlt dem Kläger für eine Unterlassungsklage das Rechtsschutzbedürfnis. 148

5. 149

Der Antrag auf Löschung „anlasslos gespeicherter" Daten (Klageanträge 8 b) und 8 c) ist aus den unter Ziffer I. 4. Genannten Gründen wegen Unbestimmtheit unzulässig. 150

6. 151

Im Übrigen ist die Klage zulässig. 152

Insbesondere sind die weitergehenden Klageanträge ausreichend bestimmt im Sinne des § 253 Abs. 2 Nr. 2 ZPO. 153

Soweit die Beklagte einwendet, dass mit dem Klageantrag zu 1 der immaterielle Schadensersatz auf verschiedene Streitgegenstände gestützt werde, greift dies nicht durch, da es sich in der Gesamtschau tatsächlich nur um einen Lebenssachverhalt handelt (vgl. LG Bochum, Urteil vom 05.05.2023- 3 O 116/22). Der Kläger macht Ansprüche aufgrund im April 154

2019 gemäß seiner Darlegung durch Datenschutzverstöße der Beklagten über W. öffentlich gewordene Daten geltend.

II. 155

Dem Kläger stehen die mit den Anträgen 1) ,2), 3), 5), 7c), 8a) und 8b) verfolgten Ansprüche nicht zu. 156

1. 157

Dem Kläger steht zunächst kein Anspruch auf immateriellen Schadenersatz entsprechend dem Klageantrag zu 1) für die vermeintlichen Datenschutzverstöße der Beklagten zu. Ein solcher Anspruch gegen die Beklagte ergibt sich weder aus Art. 82 Abs. 1 P. noch aufgrund vertraglicher Grundlage oder aufgrund sonstiger Vorschriften. 158

Insoweit kann dahinstehen, ob bzw. inwieweit eine Verletzung der P. durch die Beklagte gegenüber dem Kläger vorliegt. Denn jedenfalls fehlt ein ersatzfähiger Schaden des Klägers im Sinne des Art. 82 Abs. 1 P.. 159

Der bloße Verstoß gegen Bestimmungen der P. reicht nicht aus, um einen Schadensersatzanspruch zu begründen, vielmehr ist daneben ein der betroffenen Person entstandener Schaden und ein Kausalzusammenhang zwischen der rechtwidrigen Verarbeitung personenbezogener Daten und diesem Schaden erforderlich (EuGH, C-300/21, Urt. v. 04.05.2023). 160

Ein dem Kläger entstandener immaterieller Schaden ist nicht substantiiert dargelegt. 161

Der Kläger hat diesbezüglich keinerlei tatsächliche Umstände angeführt, mit denen er dieses Vorbringen substantiiert hätte. Er hat nicht einmal beispielhaft die von ihm geltend gemachten unbekannten Kontaktversuche via SMS oder E-Mail mit Nachrichten mit offensichtlichen Betrugsversuchen und potenziellen Virenlinks vorgelegt oder ausgeführt, in welchem Zeitraum diese erfolgt sein sollen. 162

Soweit der Kläger darlegt, dass er Sorge habe, dass die veröffentlichten Daten von Kriminellen für unlautere, von ihm weiter ausgeführte, Zwecke verwendet werden könnten, steht dies im Zusammenhang mit der von ihm geltend gemachten unregelmäßigen unbekannten Kontaktversuchen durch SMS und E-Mail. Insoweit fehlt jedoch die Darlegung jeglicher tatsächlichen Umstände durch den Kläger, durch die dieses Vorbringen substantiiert wird. Es fehlt hierzu eine konkrete Darlegung, seine Darlegung beschränkt sich auf allgemeine Ausführungen. 163

Vielmehr hat der Kläger nur vorgetragen, er sei durch die SMS- und E-Mails verärgert. 164

Auch die neuste Rechtsprechung des EUGH führt nicht zu einer Reduzierung der Anforderungen. Insoweit hat das OLG Hamm in dem Beschluss vom 21.12.2023 – 7 U 137/23 ausgeführt: „Dem folgend sieht der Senat somit den Kläger zutreffend in der Pflicht, den Indizienbeweis zum Eintritt eines kausalen immateriellen Schadens zu führen. Indem der Senat sich mit den vom Kläger dargelegten Indizien befasst und diese (hier als nicht den Eintritt eines kausalen immateriellen Schadens tragend) würdigt, setzt der Senat schlicht die weitere Vorgabe des EuGH um; denn danach ist das angerufene nationale Gericht, wenn sich eine Person auf die Befürchtung beruft, dass ihre personenbezogenen Daten in Zukunft aufgrund eines solchen Verstoßes missbräuchlich verwendet werden, gehalten zu prüfen, ob diese Befürchtung unter den gegebenen besonderen Umständen und im Hinblick auf die 165

betroffene Person als begründet angesehen werden kann.“

Unter Anlegung dieses Maßstabes kann das Gericht mangels konkreter Darlegung gerade nicht feststellen, inwieweit die Befürchtung des Klägers begründet ist. 166

Auf die mangelnde Darlegung hat bereits die Beklagte in der Klageerwiderung hingewiesen. 167

Aufgrund des Fehlens eines Schadens kommen auch vertragliche Schadensersatzansprüche oder deliktische Ansprüche nicht in Betracht. 168

2. 169

Auch betreffend den Klageantrag zu 2) steht dem Kläger kein Anspruch auf immateriellen Schadenersatz wegen der behaupteten anlasslosen Überwachung des W.-Messenger-Dienstes sowie des Sammelns und Nutzens von „Off-W.-Daten“ zu. 170

Ein solcher Anspruch gegen die Beklagte ergibt sich weder aus Art. 82 Abs. 1 P. noch aufgrund vertraglicher Grundlage oder aufgrund sonstiger Vorschriften. 171

a. 172

Der Kläger hat insoweit schon nicht schlüssig dargelegt, woraus sich ergeben soll, dass die Beklagte die über den W.-Messenger-Dienst ausgetauschten Inhalte systematisch automatisiert überwacht im Sinne eines „crawlings" der Inhalte. 173

Aus der Datenschutzrichtlinie der Beklagten ergibt sich solches jedenfalls nicht. Die Beklagte hat vielmehr plausibel dargelegt, dass sie die übertragenen Nachrichten entsprechend der gesetzlichen Vorgaben, insbesondere der ePrivacy-Richtlinie, behandelt und ein zulässiges CSAM (child sexual abuse material)-Scanning zur Identifikation kinderpornographischer Inhalte durchführt. Soweit der Kläger die Länge und Unübersichtlichkeit der Datenschutzrichtlinie der Beklagten rügt, lässt sich kein Verstoß gegen Art. 13, 14 P. erkennen. die umfangreichen datenschutzrechtlichen Anforderungen, die von Rechts wegen an die Beklagte gestellt werden, in Verbindung mit der Komplexität der von der Beklagten zur Verfügung gestellten Dienstleistungen lassen keine knappere oder einfachere Darstellung der datenschutzrechtlichen Rahmenbedingungen zu (vgl. Endurteil des Landgerichts Passau vom 16.02.2024 – 1 O 616/23). 174

b. 175

Auch betreffend das Sammeln und Nutzen der „Off-W.-Daten“ hat der Kläger einen Verstoß der Beklagten nicht ausreichend dargelegt. 176

Die Verarbeitung von Daten im Zusammenhang mit „Aktivitäten außerhalb der T.-Technologien" („Off-W.-Daten") ist durch die Einwilligung des Nutzers gedeckt, Art. 6 Abs. 1 Buchst. a und Art. 9 Abs. 2 Buchst. a P.. 177

Nach dem Vortrag der Beklagten, den der Kläger nicht bestritten hat, holt sie die Einwilligung der Nutzer mittels eines „Cookie-Banners“ ein. Die entsprechenden Einstellungen werden durch Hinweise nachvollziehbar beschrieben und können vom Benutzer nachträglich abgeändert werden. 178

Der Kläger ist bei „G." angemeldet, so dass er selbst die entsprechenden Einstellungen vornehmen kann. 179

3. 180

Der Kläger hat auch keinen Anspruch auf immateriellen Schadensersatz wegen der Weitergabe personenbezogener Daten in die USA, u.a. an die I.. 181

Ein solcher Anspruch folgt auch nicht aus Art 82 P.. 182

Eine rechtswidrige Datenübermittlung kann das Gericht nicht erkennen. Die Plattform „G." und der T.-Konzern stammen aus den USA. „ W." ist als globale Plattform konzipiert. Um dieses weltweite Netzwerk unterhalten zu können, müssen zwangsläufig Daten international ausgetauscht werden. Dass in diesem Zusammenhang auch Daten durch die Beklagte in die USA übermittelt werden, liegt folglich nahe. Dieses Erfordernis ist auch unabhängig davon, ob die Klagepartei mit US-amerikanischen „G."-Nutzern „ befreundet" ist oder nicht. Denn allein die Suche nach Nutzern in anderen Rechtsgebieten kann nur funktionieren, wenn ein grenzüberschreitender Datenaustausch stattfindet. All dies muss jedem „G."-Nutzer, auch dem Kläger, hinlänglich bekannt sein. 183

Aus dem Klagevorbringen ergibt sich auch nicht, warum die Beklagte die Daten des Klägers nicht ausreichend schützt 184

Auch die potentielle Weitergabe von Daten unter anderem an die I. begründet keinen Verstoß gegen die P.. Soweit US-Regierungsbehörden einschließlich der Geheimdienste von N.., nach US-amerikanischem Recht Auskünfte verlangen können, ist dies Folge der rechtmäßigen Datenübermittlung in den Herrschaftsbereich der Vereinigten Staaten von Amerika. Diese Möglichkeit steht der Gewährleistung eines im Wesentlichen gleichen Schutzniveaus nicht entgegen, da sie auch unter europäischem Datenschutzregime nach Art. 6 Abs. 1 Buchst. c P. (Erfüllung einer rechtlichen Verpflichtung) zulässig wäre (LG Passau aaO.). 185

Zudem hat der Kläger auch insoweit einen kausalen Schaden nicht ausreichend substantiiert dargelegt. 186

4. 187

Der Kläger hat auch keinen Anspruch auf weiteren immateriellen Schadensersatz wegen Nichterteilung einer den gesetzlichen Anforderungen entsprechenden Datenauskunft im Sinne des Art 15 P. gem. Art. 82 P.. 188

Die Beklagte hat dem Kläger gegenüber mit Schreiben vom 20.09.2023 und vom 08.01.2023 alle erforderlichen Auskünfte erteilt. 189

In dem Schreiben vom 20.09.2023 hat die Beklagte die betroffenen Datenpunkte des Klägers mitgeteilt. 190

Aus dem weiteren Schreiben der Beklagten vom 08.01.2023 ergeben sich insbesondere Hinweise auf den Umgang der „Off-W.-Daten“ und die Regulierung durch den Kläger. 191

Schließlich hat der Kläger einen Schaden im Sinne des von Art. 82 P. nicht dargelegt. Eine etwaige Ungewissheit über die Verarbeitung der eigenen Daten durch unbekannte Dritte genügt, insbesondere auch unter Berücksichtigung der dem Kläger ohnehin bereits zu dem Scraping-Vorfall vorliegenden Informationen, insoweit nicht. 192

5. 193

Auch der Unterlassungsantrag (Klageantrag 7 c) hinsichtlich der Übermittlung personenbezogener Daten des Klägers in die USA, insbesondere an die F. (I.) ist unbegründet. 194

Eine rechtswidrige Datenübermittlung ist nicht schlüssig dargelegt. Die Plattform „G." und der T.-Konzern stammen aus den USA. „ W." ist als globale Plattform konzipiert. Um dieses weltweite Netzwerk unterhalten zu können, müssen zwangsläufig Daten international ausgetauscht werden. Dass in diesem Zusammenhang auch Daten durch die Beklagte in die USA übermittelt werden, liegt folglich nahe. Dieses Erfordernis ist auch unabhängig davon, ob die Klagepartei mit US-amerikanischen „G."-Nutzern „ befreundet" ist oder nicht. Denn allein die Suche nach Nutzern in anderen Rechtsgebieten kann nur funktionieren, wenn ein grenzüberschreitender Datenaustausch stattfindet. All dies muss jedem „G."-Nutzer, auch der Klagepartei, hinlänglich bekannt sein. Die Klagepartei hat keinen Anspruch darauf, dass „ G." dergestalt betrieben wird, dass sämtliche Daten in Europa gespeichert und verarbeitet werden im Sinne eines rein europäischen „ G.". Die unternehmerische Entscheidung des Betreibers der Plattform „G.", Daten in den Vereinigten Staaten von Amerika zu verarbeiten, ist von den Nutzern hinzunehmen, zumal niemand dazu gezwungen wird, die Plattform „G." zu nutzen. 195

Um dieses weltweite Netzwerk unterhalten zu können, müssen zwangsläufig Daten international ausgetauscht werden. Dass in diesem Zusammenhang auch Daten durch die Beklagte in die USA übermittelt werden, liegt folglich nahe. Dieses Erfordernis ist auch unabhängig davon, ob die Klagepartei mit US-amerikanischen „G."-Nutzern befreundet" ist oder nicht. Denn allein die Suche nach Nutzern in anderen Rechtsgebieten kann nur funktionieren, wenn ein grenzüberschreitender Datenaustausch stattfindet. All dies muss jedem „G."-Nutzer, auch der Klagepartei, hinlänglich bekannt sein. Der Kläger hat auch keinen Anspruch darauf, dass „G." dergestalt betrieben wird, dass sämtliche Daten in Europa gespeichert und verarbeitet werden im Sinne eines rein europäischen „G.". Die unternehmerische Entscheidung des Betreibers der Plattform „G.", Daten in den Vereinigten Staaten von Amerika zu verarbeiten, ist von den Nutzern hinzunehmen, zumal niemand dazu gezwungen wird, die Plattform „ G." zu nutzen. 196

Soweit US-Regierungsbehörden einschließlich der Geheimdienste von N.., nach US-amerikanischem Recht Auskünfte verlangen können, ist dies Folge der rechtmäßigen Datenübermittlung in den Herrschaftsbereich der Vereinigten Staaten von Amerika. Diese Möglichkeit steht der Gewährleistung eines im Wesentlichen gleichen Schutzniveaus nicht entgegen, da sie auch unter europäischem Datenschutzregime nach Art. 6 Abs. 1 Buchst. c P. (Erfüllung einer rechtlichen Verpflichtung) zulässig wäre (vgl. zu dem Vorstehenden: Urteil des Landgerichts Passau aaO.). 197

6. 198

Der Kläger hat gegen die Beklagte keine weitergehenden Auskunftsansprüche gem. Art 15 P. mehr. 199

a. 200

Soweit der Kläger gemäß dem Klageantrag zu 8 a) Auskunft hinsichtlich der ihn betreffenden 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 Kontakt-Import-Tools erlangt werden konnten, ist dieser Anspruch bereits gem. § 362 BGB erfüllt. 201

Denn die Beklagte hat dem Kläger mit Schreiben vom 20.09.2023 ausreichend Auskunft zu den abgegriffenen Daten erteilt. 202

b. 203

Auch ein weiterer Anspruch auf Auskunftserteilung über die überwachten, ausgewerteten, gespeicherten Daten „aus der Überwachung des W.-Messengers", „Chat-Protokolle vorzulegen und deren interne Bewertung offenzulegen", besteht nicht. Nach dem unbestrittenen Vortrag der Beklagten kann der Kläger die Chat-Verläufe selbst herunterladen. Dies hat die Beklagte in ihrem Schreiben vom 08.01.2024 ausreichend dargestellt. 204

Der Auskunftsanspruch ist dadurch erfüllt, § 362 Abs. 1 BGB. Was unter einer „internen Bewertung" zu verstehen sein soll, erschließt sich dem Gericht nicht; eine Subsumtion unter eine der Kategorien des Art. 15 Abs. 1 P. ist insoweit nicht möglich. 205

c. 206

Soweit Auskunft begehrt wird, welche „Off-W.-Daten" durch die Beklagte an der IP-Adresse der Klägerseite gesammelt und zu welchem Zweck sie gespeichert und verwendet wurden, verweist die Beklagte in ihrem vorgerichtlichen Schreiben vom 08.01.2024 ebenfalls zu Recht auf die von ihr zur Verfügung gestellte Selbstauskunftsmöglichkeit und hinsichtlich der Verarbeitungszwecke auf eine bestimmte Seite im Hilfebereich. Die Auskunft ist damit erteilt, § 362 Abs. 1 BGB. 207

d. 208

Hinsichtlich etwaiger an die I. übermittelter Daten kann die Beklagte die Auskunft verweigern, weil zum einen eine Geheimhaltungspflicht nach US-amerikanischem Rechts besteht und es sich zum anderen um ihrem Wesen nach geheimhaltungsbedürftige Informationen handelt, Art. 23 P. i.V.m. § 29 Abs. 1 S. 2 BDSG, wobei sich letztgenannte Vorschrift entgegen der Auffassung der Klagepartei schon dem Wortlaut nach nicht auf Berufsgeheimnisträger beschränkt. Es versteht sich von selbst, dass die Information, ob und welche Auskünfte an Geheimdienste erteilt werden, ihrem Wesen nach geheimhaltungsbedürftig ist (vgl. LG Passau aaO.). 209

III. 210

Mangels Hauptanspruchs hat der Kläger auch keinen Anspruch auf Ersatz von vorgerichtlichen Rechtsanwaltskosten. 211

IV. 212

Dem Kläger war keine Schriftsatzfrist gem. § 139 Abs. 5 ZPO zu gewähren. 213

Kann die Partei im Termin nicht sofort eine Erklärung zu gerichtlichen Hinweisen abgeben, dh notwendigenfalls ihren Vortrag ergänzen oder präzisieren, so ist die Verhandlung zu vertagen, gegebenenfalls ins schriftliche Verfahren zu wechseln, oder der Partei ist auf Antrag ein befristetes Schriftsatzrecht einzuräumen (vgl. Musielak/Voit/Stadler, 21. Aufl. 2024, ZPO § 139 Rn. 29). 214

Hinweise des Prozessgegners lassen die gerichtliche Hinweispflicht nicht ohne weiteres entfallen. Nur wenn die Partei durch eingehenden und von ihr erfassten Vortrag der Gegenpartei zutreffend über die Sach- und Rechtslage unterrichtet war, bedarf es keines 215

erneuten richterlichen Hinweises (Greger in: Zöller, Zivilprozessordnung, 35. Auflage 2024, § 139 ZPO, Rn. 7).

Unter Anwendung dieser Maßstäbe waren weitere Hinweise des Gerichts nicht erforderlich. Denn die Beklagte hat mit Schriftsätzen vom 01.02.2024 und 20.03.2024 umfangreich auf die entsprechenden rechtlichen Probleme hingewiesen und eine Vielzahl an Gerichtsentscheidungen beigefügt. Auf diesen Vortrag hat der Kläger nicht mehr reagiert, sodass insbesondere auch einige streiterhebliche Tatsachen unstreitig geblieben sind. 216

Zudem ist zu berücksichtigen, dass es sich vorliegend um eine Masseverfahren mit immer wiederkehrenden Rechtsfragen handelt, auf die sich die mit dieser Thematik vertrauten Parteivertreter im Vorfeld einstellen können. 217

V. 218

Die Kostenentscheidung folgt aus § 91 ZPO. 219

Die Entscheidung hinsichtlich der vorläufigen Vollstreckbarkeit ergibt sich aus § 709 ZPO. 220

Justiz NRW
Rechtsprechungsdatenbank ONLINE