Gericht:	Thüringer Oberlandesgericht 3. Zivilsenat
Entscheidungsdatum:	17.11.2025
Aktenzeichen:	3 U 885/24
Dokumenttyp:	Urteil
Quelle:	juris
Normen:	Art 4 Nr 14 EUV 2016/679, Art 9 Abs 1 EUV 2016/679, Art 9 Abs 2 Buchst a EUV 2016/679, Art 82 Abs 1 EUV 2016/679

Umfang des datenschutzrechtlichen Schadensersatzes bei Nutzung von Gesichtserkennungssoftware ohne Einwilligung für Online-Prüfungen einer Hochschule

Leitsatz

Der automatisierte Abgleich eines zuvor aufgenommenen Referenzbildes des Gesichts eines Prüfungskandidaten mit während einer Online-Prüfung aufgenommenen Bildern zur Feststellung möglicher Täuschungsversuche stellt eine Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person dar, die gemäß Art. 9 Abs. 1 DSGVO grundsätzlich untersagt ist und Ansprüche auf immateriellen Schadensersatz gemäß Art. 82 Abs. 1 DSGVO begründen kann. Wählt der Prüfungskandidat unter mehreren zur Verfügung stehenden Möglichkeiten der Prüfungsdurchführung die der Online-Prüfung, liegt allein darin keine ausdrückliche Einwilligung mit der Verarbeitung seiner biometrischen Daten im Sinne von Art. 9 Abs. 2 Buchst. a DSGVO.(Rn.62) (Rn.63)

Orientierungssatz

1. Durch die unzulässige Verarbeitung der biometrischen Daten der Studentin bei der Durchführung der Online-Prüfungen ist dieser ein nicht allzu intensiv einzuschätzender Schaden in Form einer psychischen Beeinträchtigung entstanden, für den die Hochschule gemäß Art. 82 Abs. 1 DSGVO Ersatz zu leisten hat. Die Höhe des durch die erlittene psychische Beeinträchtigung entstandenen immateriellen Schaden bemisst das Gericht mit einem Betrag von 200 EUR.(Rn.66) (Rn.69)

2. Der bloße Kontrollverlust über personenbezogene Daten bei dem von einem Datenschutzverstoß Betroffenen stellt bereits einen ersatzfähigen Schaden dar, wenn der Eintritt eines solchen Kontrollverlusts dargelegt und gegebenenfalls bewiesen wird. Der Datenschutzverstoß als solcher stellt noch keinen Nachweis eines Kontrollverlusts dar (Anschluss BGH, Urteil vom 18. November 2024 - VI ZR 10/24).(Rn.70)

3. Ein Kontrollverlust durch die Verarbeitung der biometrischen Daten scheidet aus, wenn die betroffene Person zum Zeitpunkt der Datenverarbeitung bereits keine Kontrolle mehr über ihre ihr Gesicht betreffenden biometrischen Daten gehabt hat. Dies ist der Fall, wenn wie vorliegend die Studentin seit einigen Jahren Fotos von ihrem Gesicht auf stark besuchten Internetplattformen, insbesondere Instagram, veröffentlicht hat. Damit bestand für eine unbegrenzte Vielzahl von Nutzern der Plattform Instagram über eine lange Zeitdauer die potentielle Möglichkeit, aus den Gesichtsfotos der Klägern biometrische Daten zu gewinnen. Der Umstand, dass die Generierung und Nutzung von biometrischen Daten aus den von ihr veröf-

fentlichten Bildern regelmäßig rechtswidrig sein dürfte, ändert am Eintritt des Kontrollverlusts nichts.(Rn.71)

Verfahrensgang

vorgehend LG Erfurt 8. Zivilkammer, 23. Oktober 2024, 8 O 1117/22

Tenor

1. Auf die Berufung der Klägerin wird das Urteil des Landgerichts Erfurt vom 23.10.2024, Az. 8 O 1117/22, abgeändert:

   Die Beklagte wird verurteilt, an die Klägerin einen immateriellen Schadensersatz in Höhe von 200,00 EUR zu zahlen. Im Übrigen wird die Klage abgewiesen.

2. Die weitergehende Berufung wird zurückgewiesen.

3. Von den Kosten des Rechtsstreits hat die Klägerin 80 % und die Beklagte 20 % zu tragen.

4. Das Urteil ist vorläufig vollstreckbar.

5. Die Revision wird nicht zugelassen.

Gründe

I.

1 Die Klägerin begehrt von der Beklagten, einer als Körperschaft des öffentlichen Rechts organisierten Hochschule, immateriellen Schadensersatz für behauptete Verstöße gegen datenschutzrechtliche Bestimmungen im Zusammenhang mit der Durchführung von Online-Prüfungen.

2 Die Klägerin absolvierte in den Jahren 2020 bis 2022 an der beklagten Hochschule den Studiengang „Master of Education Grundschule“. Aufgrund der gesetzlichen Kontaktbeschränkungen nach Ausbruch der Covid-19-Pandemie erließ die Beklagte eine sogenannte „Corona-Satzung“ (Satzung der U. zur Erweiterung und Änderung der Prüfungsformen und Formen von Lehrveranstaltungen in Prüfungs- und Studienordnungen aufgrund von Einschränkungen durch die Corona-Pandemie vom 25.06.2020), die für die Studenten die Möglichkeit vorsah, auf Antrag in verschiedener Weise Prüfungen per Fernklausur abzulegen. Mit Schreiben der Beklagten wurde den Studenten die Möglichkeit eingeräumt folgende Anträge zu stellen:

1.

3 *Studierenden, die nicht über die für eine elektronische Fernprüfung benötigte technische Ausstattung (geeignetes IT-Endgerät, Webkamera, Betriebssystem, Software) verfügen, wird in dem der Universität zur Verfügung stehenden Umfang die Ausstattung – mit Ausnahme von Webkameras – auf begründeten Antrag von der Universität übergangsweise für die Teilnahme an der Prüfung bereitgestellt. Hierzu werden im Regelfall EDV-Poolarbeitsplätze der Universität zugewiesen.*

2.

4 *Studierende, die nicht über eine geeignete Webkamera verfügen, absolvieren die elektronische Prüfung (E-Klausur) am eigenen IT-Endgerät unter Aufsicht in den Räumlichkeiten der Universität.*

3.

5 *Im Falle fehlender oder unzureichender Internetverbindung erfolgt eine Prüfungsteilnahme am eigenen IT-Endgerät in Prüfungsräumlichkeiten der Universität.*

4.

6 *Studierende, die nicht an einer elektronischen Prüfung teilnehmen möchten (pandemiebedingter Rücktritt), können die Prüfung in der von der jeweiligen Studien- und Prüfungsordnung vorgesehenen Prüfungsform ablegen, sobald die Infektionsschutzmaßnahmen im Sinne von § 2 Abs. 1 dem nicht mehr entgegenstehen.*

7 Im Weiteren wurden fünf Auswahlmöglichkeiten zur Verfügung gestellt:

1.

8 *Ich verfüge über die technische Ausstattung (IT-Gerät, Webkamera, Internetverbindung) und absolviere die Klausur außerhalb des Campus' der Uni.*

2.

9 *Ich habe keine oder eine nur unzureichende Internetverbindung und absolviere die Klausur am eigenen IT-Endgerät in Prüfungsräumlichkeiten der Universität.*

3.

10 *Ich verfüge nicht über eine geeignete Webkamera und absolviere die Klausur am eigenen IT-Endgerät unter Aufsicht in den Räumlichkeiten der Universität.*

4.

11 *Ich verfüge nicht über die technische Ausstattung und muss die Klausur an einem Gerät der Universität absolvieren.*

5.

12 *Ich trete pandemiebedingt von der elektronischen Prüfung zurück und werde die Prüfung in der von der jeweiligen Studien- und Prüfungsordnung vorgesehenen Prüfungsform ablegen, sobald die Infektionsschutzmaßnahmen im Sinne von § 2 Abs. 1 dem nicht mehr entgegenstehen.“*

13 Die Klägerin gab gegenüber der Beklagten an, dass sie die Auswahlmöglichkeit 1 in Anspruch nehmen wolle.

14 Zur Durchführung der Online-Prüfungen außerhalb des Universitätscampus bediente sich die Beklagte der Software „WISEflow“ des Anbieters Uniwise ApS. Diese Software ist über einen Internetbrowser aufzurufen. Auf der aufgerufenen Internetseite waren sogenannte Google Tag Manager installiert, um bestimmte Webseitenfunktionen technisch zu ermöglichen.

15 Die Software „WISEflow“ verwendet zur Verhinderung von Prüfungsbetrug eine Funktion der automatischen Gesichtserkennung der Prüfungsteilnehmer. Dabei wird vor den Prüfungen - bei der Klägerin erfolgte dies am 09.07.2020 - ein Referenzbild des Prüfungsteilnehmers angefertigt, wobei bestimmte Punkte des Gesichts durch das Programm zueinander ins Verhältnis gesetzt werden (biometrische Aufnahme). Die Klägerin nahm zwischen Juni 2020 und Februar 2021 unter Anwendung der oben beschriebenen Software an 12 Fernprüfungen teil, wobei es sich teilweise um Probeklausuren handelte. Während der Prüfung wurden dabei mittels der Webkamera des Endgeräts der Klägerin in unregelmäßigen Abständen Bilder des Gesichts der Klägerin angefertigt und diese mit dem am 09.07.2020 erstellten Referenzbild verglichen, wobei die Software einen Übereinstimmungswert ermittelte. Die Software war so programmiert, dass bei einer Unterschreitung des Übereinstimmungswertes von 99 % eine Meldung ausgegeben wurde, die den aufsichtsführenden Prüfer veranlassen sollte, dem betroffenen Prüfling Gelegenheit zur Stellungnahme zu der Abweichung einzuräumen und gegebenenfalls ein Verfahren wegen möglichen Prüfungsbetruges einzuleiten. Bei den von der Klägerin durchgeführten Onlineprüfungen kam es zu keiner solchen Unterschreitung des Referenzwertes. Die Gesichtserkennung wurde durch den in WISEflow integrierten Dienst Amazon Rekognition durchgeführt, der von einer in Luxemburg ansässigen Tochtergesellschaft Amazon Web Services EMEA S.a.r.l. der in den USA residierenden Amazon Web Services Inc. betrieben wird.

16 Zusätzlich zur Duldung der Gesichtserkennung waren die Prüfungsteilnehmer verpflichtet, einen sogenannten Lock-Down-Browser des Anbieters Respondus auf ihrem Endgerät zu installieren, welcher zur Verringerung möglicher Betrugsversuche verschiedene Funktionen des Endgeräts der Prüflinge, insbesondere das Aufrufen von in der Prüfung nicht gestatteten Internetseiten sowie das Drucken, Kopieren und das Einfügen von Inhalten sperrte. Zudem wurde mit der Verwendung der Software WISEflow auch der Google Tag Manager auf dem Endgerät der Klägerin installiert, der zumindest eine Übersendung der IP-Adresse, von der die Klägerin das Internet nutzte, an die Firma Google Ireland Ltd. bewirkte. Ob darüber hinaus eine Übersendung an die in den USA ansässige Firma Google LLC erfolgte, ist zwischen den Parteien streitig.

17 Die Klägerin ist seit 2015 in den sozialen Netzwerken aktiv und hat dort, insbesondere auf der Plattform Instagram, auch Fotos ihres Gesichts hochgeladen. Seit 2022 sind die Beiträge der Klägerin auf Instagram nur noch für einen eingeschränkten Personenkreis sichtbar. Zudem hat die Klägerin bei dem Dienst Google Maps Bewertungen verschiedener Einrichtungen unter Verwendung ihres Klarnamens abgegeben.

18 Die Klägerin hat behauptet, dass die Verwendung der automatischen Gesichtserkennung sie unter erheblichen Stress gesetzt habe, da sie stets in Angst gewesen sei, durch bestimmte Verhaltensweisen, etwa dem Schauen aus dem Fenster, in den Verdacht eines Prüfungsbetrugs zu geraten. Zudem befürchte sie, dass durch die Verwendung des Lock-Down-Browsers Zugriff auf die auf ihrem Endgerät gespeicherten Daten genommen werden konnte.

19 Sie meint, dass die Beklagte durch die Durchführung der Online-Prüfungen in mehrfacher Hinsicht gegen die Vorschriften der DSGVO, insbesondere gegen Art. 9, 22 und 44 DSGVO verstoßen habe. Zudem liege ein Verstoß gegen § 15 TMG a.F. bzw. 25 Abs. 1 Satz 2 TTDSG vor. Eine wirksame Einwilligung in die Verletzung ihrer Datenschutzrechte sei nicht erfolgt. Für die von ihr infolge der Verstöße durch die Beklagte erlittenen Beein-

trächtigungen sei die Zahlung eines Schmerzensgeldes von mindestens 1.000 EUR angemessen.

20 Die Klägerin hat beantragt,

21 die Beklagte zu verurteilen, an die Klägerin einen angemessenen immateriellen Schadenersatz zu zahlen, dessen Höhe in das Ermessen des Gerichts gestellt wird, der jedoch mindestens 1.000,00 € beträgt.

22 Die Beklagte hat beantragt,

23 die Klage abzuweisen.

24 Sie ist der Auffassung, dass sie nicht gegen datenschutzrechtliche Bestimmungen verstoßen habe. Zudem habe die Klägerin durch die Teilnahme an der Online-Prüfung in Kenntnis der ihr zur Verfügung stehenden Alternativangebote in die Verfahrensweise eingewilligt. Durch die Verwendung des Lock-Down-Browsers sei kein Zugriff auf die auf dem Endgerät der Klägerin gespeicherten Daten erfolgt. Eine Übermittlung von Daten an Drittstaaten außerhalb der EU, insbesondere an die in den USA ansässige Muttergesellschaft des Dienstleisters, welcher die Gesichtserkennung durchgeführt hat, sei nicht erfolgt, aber auch nicht an die Firma Google LLC. Durch die Verwendung des Google Tag Managers sei lediglich die IP-Adresse, mit der die Klägerin das Internet genutzt habe, übermittelt worden. Hierbei handele es sich nicht um personenbezogene Daten, da eine IP-Adresse nicht einem einzelnen Nutzer zugeordnet sei und der Internetanschluss, von dem sie die Prüfung durchgeführt habe, nicht auf sie ausgestellt worden sei. Zudem sei der Beklagten kein immaterieller Schaden entstanden.

25 Das Landgericht hat nach persönlicher Anhörung der Klägerin mit Urteil vom 23.10.2024, welches ihr am 30.10.2024 zugestellt worden ist, die Klage abgewiesen. Ein Schadensersatzanspruch aus Art. 82 DSGVO komme nicht in Betracht, wobei offenbleiben könne, ob der Einsatz der Gesichtserkennungssoftware gegen Art. 9 DSGVO verstoße, insbesondere ob ein Fall des Art. 9 Abs. 2 DSGVO der ausnahmsweisen Zulässigkeit der Verarbeitung biometrischer Daten vorliege. Die Klägerin habe die ihr obliegende Darlegung und den Nachweis eines ihr entstandenen Schadens nicht erbracht. Zwar müsse der der betreffenden Person entstandene Schaden nicht einen bestimmten Grad der Erheblichkeit erreichen, jedoch müsse ein Schaden überhaupt entstanden sein, wozu nicht bereits die Verletzung der Freiheit der Person, die sie betreffenden Daten zu kontrollieren, ausreichend sei. Einen solchen Schaden habe die Klägerin auch bei ihrer persönlichen Anhörung durch die Kammer nicht dargelegt. Soweit sie dargelegt habe, dass sie sich durch die Gesamtsituation der Prüfung, insbesondere durch den Umstand, dass sie hierbei auf sich allein gestellt gewesen sei, belastet gefühlt habe, stehe dies in keinem Zusammenhang mit einem etwaigen Datenschutzverstoß durch die Beklagte. Zwar habe die Klägerin ausgeführt, dass sie während der Prüfung verunsichert gewesen sei, dass durch die Kameraüberwachung, deren Art und Weise ihr unbekannt gewesen sei, ihr Verhalten leicht als Betrugsversuch ausgelegt werden könnte. Sie habe jedoch ebenso erklärt, dass sie darüber informiert gewesen sei, dass ein Referenzbild von ihr erstellt werde, was sie nicht dazu veranlasst habe, weitere Nachforschungen über das genaue Procedere der Onlineüberwachung anzustellen, was ihr möglich gewesen wäre. Bei der Kammer habe sich daher nicht die Überzeugung bilden können, dass die Klägerin aufgrund des Einsatzes der Gesichtserkennungssoftware ein Leiden oder einen Kontrollverlust hinsichtlich ihrer Daten verspürt habe. Es müsse aufgrund der Angaben der Klägerin davon ausgegan-

gen werden, dass sie auch bei einer Videoüberwachung ohne den Einsatz einer Software zur Verarbeitung biometrischer Daten die Sorge verspürt habe, von den Prüfern durch ihr Verhalten eines Betrugsversuchs verdächtigt werden zu können.

26 Ein Verstoß gegen Art. 22 DSGVO sei nicht anzunehmen, da eine Entscheidung mit rechtlicher Wirkung gerade nicht ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung basiere. Vielmehr liege in dem Procedere nach einem festgestellten Unterschreiten des Grenzwertes von 99 % noch keine rechtlich verbindliche Entscheidung, da der Prüfer nach Einräumung einer Gelegenheit zur Stellungnahme durch den Prüfling zu entscheiden habe, ob ein Täuschungsversuch in Betracht komme und ein Prüfungsverfahren einzuleiten sei. Allein die Feststellung eines Übereinstimmungswertes von weniger als 99 % durch die Software habe für die Klägerin noch keine rechtlich wirksame oder ähnlich beeinträchtigende Entscheidung bedeutet.

27 Es könne auch offenbleiben, ob die Verwendung des Lock-Down-Browsers zur Speicherung von Daten auf dem Endgerät der Klägerin geführt hat oder ob hierdurch auf dem Gerät gespeicherte Informationen ausgelesen wurden. Zwar habe die Klägerin glaubhaft versichert, dass sie sich Gedanken über den Datenzugriff auf ihren Laptop gemacht habe. Sie habe jedoch nicht plausibel erklärt, warum - auch angesichts ihres sonstigen Umgangs mit persönlichen Daten - bei ihr ein immaterieller Schaden in Form eines Kontrollverlusts entstanden sei. Es sei nicht ersichtlich, warum durch die Installation des Lock-Down-Browsers eine gesteigerte Besorgnis eines Datenzugriffs entstanden sei. Auch durch ihr nachträgliches Verhalten sei die Annahme derartiger Befürchtungen nicht gerechtfertigt, da sie den Laptop, wenn auch umfangmäßig reduziert, weiterhin nutze.

28 Dass die Klägerin eine messbare Besorgnis wegen einer möglichen unzulässigen Übermittlung von Daten an Drittstaaten spürte, sei aufgrund ihrer Nutzung etwa von Angeboten der Firmen Google und Meta, bei der sich eine Übermittlung von Daten an Drittstaaten nur mit erheblichem Aufwand vermeiden lasse, nicht naheliegend.

29 Auch ein Anspruch aus § 839 BGB i.V.m. Art. 34 GG unter dem Aspekt der Verletzung des allgemeinen Persönlichkeitsrechts komme nicht in Betracht. Es fehle insoweit an einem - anders als bei nach Art. 82 DSGVO - erforderlichen schweren Eingriff in das Persönlichkeitsrecht. Zwar bestehe zwischen der Beklagten und der Klägerin ein gewisses Machtgefälle, welches es der Klägerin erschwert habe, sich der Teilnahme an der Online-Prüfung zu entziehen. Andererseits habe die Beklagte durch die Einräumung der Online-Prüfungen es den Studenten ermöglicht, ihr Studium trotz der Beschränkungen durch die Covid-19-Pandemie zeitnah fortzusetzen oder abzuschließen. Die Beklagte habe daher die Online-Prüfungen nicht zu ihrem Vorteil genutzt.

30 Auch aufgrund des bisherigen Nutzerverhaltens der Klägerin erscheine ein etwaiger Eingriff in deren Persönlichkeitsrecht daher nicht als schwerwiegend.

31 Gegen dieses Urteil hat die Klägerin am 02.12.2024 Berufung eingelegt, die sie am 27.12.2024 begründet hat und mit der sie ihren erstinstanzlichen Klageantrag vollumfänglich weiterverfolgt.

32 Die Klägerin moniert, dass das Landgericht zu Unrecht das Vorhandensein eines immateriellen Schadens bei der Klägerin abgelehnt habe und infolgedessen nicht zu der Frage gelangt sei, ob die Durchführung der Online-Prüfungen rechtswidrig gewesen sei.

33 Das Landgericht habe insbesondere verkannt, dass ausweislich der Leitentscheidung des BGH vom 18.11.2024, Az.: VI ZR 10/24 sowie der vorangegangenen Entscheidung des EuGH vom 04.10.2024, Az.: C-200/23, bereits ein Kontrollverlust über seine Daten einen ersatzfähigen Schaden für den von einem Datenschutzverstoß Betroffenen darstelle, ohne dass zusätzlich eine weitere immaterielle Beeinträchtigung festgestellt werden müsse. Ein solcher Kontrollverlust könne zum einen durch einen „Datendiebstahl“ etwa mittels eines Hackerangriffs oder zum anderen - wie vorliegend - durch eine unzulässige Datenverarbeitung durch den Verantwortlichen selbst entstehen. Durch die unzulässige Verarbeitung der biometrischen Daten der Klägerin sei diese zum Objekt einer illegalen Überwachungssoftware gemacht worden, was einen schwerwiegenden Grundrechtseingriff darstelle.

34 Ein schadensbegründender Kontrollverlust über ihre Daten liege zum einen in der Weitergabe der unbefugt erhobenen biometrischen Daten der Klägerin an Unternehmen der Amazon Web Service Gruppe, die die Daten ihrerseits unbefugt verarbeitet habe. Es bestünden für die Klägerin auch keine Möglichkeit, die Kontrolle über ihre biometrischen Daten wieder zu erlangen. Die Klägerin habe zuvor die Kontrolle über ihre biometrischen Daten gehabt, da sie diese nicht zuvor allgemein veröffentlicht habe. Der Umstand, dass aus den von der Klägerin im Internet veröffentlichten Bildern ihres Gesichts biometrische Daten gewonnen werden können, führe nicht dazu, dass sie die Kontrolle über ihre biometrische Daten bereits zuvor verloren hätte, da eine entsprechende Nutzung der veröffentlichten Bilder durch Dritte rechtswidrig gewesen wäre. Der Kontrollverlust werde dadurch verstärkt, dass die Beklagte widersprüchliche Angaben über die Verarbeitung der Daten gemacht habe, wodurch sie ihren datenschutzrechtlichen Rechenschaftspflichten aus Art. 5 Abs. 2 DSGVO nicht nachgekommen sei. In der Datenschutzinformation habe die Beklagte sich als Erlaubnisnorm für die Verarbeitung der biometrischen Daten zunächst auf Art. 9 Abs. 2 lit. g DSGVO i.V.m. § 11 Abs. 1 Satz 1 ThürHG, in der Klageerwiderung aber auf § 16 Abs. 2 Satz 1 Nr. 2 ThürDSG berufen. Im weiteren Verlauf des Verfahren habe sie sich auf Art. 9 Abs. 2 lit. e DSGVO berufen (vorherige Veröffentlichung biometrischer Daten durch die Klägerin) und sodann auf eine Einwilligung der Klägerin. Zudem habe die Beklagte unterschiedliche Angaben zur Löschung der Gesichtsaufnahmen (zunächst 6 Monate, dann sofortige Löschung nach Gesichtsabgleich, sodann 80 Tage) gemacht. Die Beklagte habe auch keine Vereinbarung mit der Amazon Web Services Gruppe vorgelegt, was aber gemäß Art. 28 Abs. 3, 4 DSGVO verbindlich vorgeschrieben sei. Das Landgericht habe alle diese Aspekte nicht beachtet und zu Unrecht einen Schaden abgelehnt.

35 Zudem sei ein Schaden der Klägerin aus der Verletzung ihrer Grundrechte auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts, auf Schutz der Privatsphäre sowie des Schutzes personenbezogener Daten eingetreten.

36 Der Schaden sei durch konkrete psychische Belastungen der Klägerin vertieft worden. Sie habe diese während der mündlichen Verhandlung vor dem Landgericht am 28.08.2024 anschaulich und nachvollziehbar dargelegt. Das Landgericht habe die getroffenen Feststellungen unzutreffend gewertet und dabei verkannt, dass an den Nachweis der konkreten Befürchtungen nach der höchstrichterlichen Rechtsprechung keine zu hohen Anforderungen gestellt werden dürfen. So habe die Klägerin nachvollziehbar dargelegt, dass sie aufgrund der ständigen Angst, eines Betruges bezichtigt zu werden, es nicht gewagt habe, die Augen vom Bildschirm zu lösen.

37 Ihre Befürchtungen habe die Klägerin auch in einer erstinstanzlich als Beweismittel angebotenen Sprachnachricht (vorgelegt als Audiodatei und transkribierte Niederschrift) an eine Kommilitonin dargelegt. Das Landgericht habe sich mit diesem Beweismittel gar nicht auseinandergesetzt. Die Klägerin habe eine begründete Sorge vor dem Eintritt von Risiken gehabt, die mit dem Einsatz der automatisierten biometrischen Überwachung typischerweise einhergehen. Entgegen den Ausführungen des Landgerichts habe dieses Risiko bei einer herkömmlichen Prüfungsüberwachung mittels Videoaufsicht nicht bestanden. Das Landgericht habe die Verneinung eines Schadens auch unzutreffend damit begründet, dass sie sich nicht an eine universitäre Anlaufstelle gewandt habe, um nach alternativen Prüfungsmöglichkeiten nachzufragen. Hierbei werde verkannt, dass die Voraussetzungen für eine andere Prüfungsüberwachung (Fehlen der technischen Mittel für die Onlineprüfung) bei der Klägerin gerade nicht vorlagen.

38 Das Landgericht habe sich im Urteil zwar formal zur Rechtsprechung des EuGH, wonach die Zuerkennung eines Schadensersatzanspruchs nicht vom Überschreiten einer Erheblichkeitsschwelle abhängig gemacht werden kann, bekannt, letztlich aber doch auf eine gewisse Erheblichkeit des Schadens abgestellt.

39 Das Verhalten der Beklagten begründe einen Verstoß gegen verschiedene datenschutzrechtliche Bestimmungen. Die Klägerin habe keine Einwilligung in die Verarbeitung ihrer biometrischen Daten gemäß Art. 9 Abs. 1 lit. a DSGVO durch eine unwidersprochene Teilnahme an den Onlineprüfungen erteilt, zumal Art. 9 Abs. 1 DSGVO eine ausdrückliche Einwilligung erfordere. Die Klägerin habe ihre biometrischen Daten auch nicht zuvor veröffentlicht. Die Verarbeitung sei auch nicht gemäß Art. 9 Abs. 2 lit. e DSGVO i.V.m. § 16 Abs. 2 Nr. 2 ThürDSG gestattet gewesen, da die Voraussetzung dieser Norm nicht vorgelegen hätten und diese Landesnorm zudem den Anforderungen der Öffnungsklausel der DSGVO nicht gerecht werde. Die Beklagte habe Auftragsverarbeitungsverträge weder bezüglich des Auftragsverarbeiters noch des Unterauftragsverarbeiters vorgelegt. Mit der Fa. Uniwise sei ein solcher erst am 08.11.2021 abgeschlossen worden.

40 Zudem liege ein Verstoß gegen Art. 22 Abs. 2, 4 DSGVO vor, da die Beklagte die Klägerin einer rechtswidrigen automatisierten Entscheidungsfindung unter Verwendung biometrischer Daten unterworfen habe. Soweit das Landgericht darauf abstellte, dass bei automatisierter Feststellung eines Übereinstimmungswertes von weniger als 99 % noch keine rechtliche und auch sonst keine erhebliche Beeinträchtigung vorliege, verkenne es, dass in nahezu allen anderen Sprachfassungen der DSGVO nicht von „erheblichen Beeinträchtigungen“, sondern von „erheblichen Auswirkungen“ die Rede ist. Die Entscheidung über die Einleitung oder Nichteinleitung eines Verfahrens nach der Prüfungsordnung zur Feststellung eines Täuschungsversuchs habe auch erhebliche Auswirkungen auf die Klägerin gehabt, da durch den Vorwurf des Täuschungsverdachts das Verhältnis zur Universität nachhaltig beeinflusst werden könne.

41 Darüber hinaus würden Verstöße gegen § 15 TMG a.F. (nunmehr in § 25 TDDG geregelt) vorliegen, da auf Informationen auf dem von der Klägerin genutzten Endgerät zugegriffen worden seien, ohne dass ein Einwilligung vorgelegen habe. Schließlich habe die Beklagte personenbezogene Daten der Klägerin entgegen Art. 44 ff. DSGVO in die USA übermittelt. Hierdurch sei ein Kontrollverlust der Klägerin über ihre Daten entstanden, womit sich das Landgericht nicht auseinandergesetzt habe.

42 Mit Schriftsatz vom 27.10.2025 hat die Klägerin erklärt, dass sie ihren Schadensersatzanspruch nicht mehr auf die Übermittlung von IP-Adressen an den Google Konzern stütze.

43 Die Klägerin beantragt,

44 unter Abänderung des Urteils des Landgerichts Erfurt vom 23.10.2024 die Beklagte zu verurteilen, an sie einen immateriellen Schadensersatz zu zahlen, dessen Höhe in das Ermessen des Gerichts gestellt wird, der jedoch mindestens 1.000,00 EUR beträgt.

45 Die Beklagte beantragt,

46 die Berufung zurückzuweisen.

47 Sie meint, die Berufung sei bereits unzulässig, da sich die Berufungsbegründung nicht hinreichend mit dem Urteil des Landgerichts, insbesondere mit den Ausführungen zur Frage zwischen der Kausalität einer vermeintlichen Rechtsverletzung und einem Schaden, namentlich in Form eines Kontrollverlusts, auseinandergesetzt habe.

48 Die Berufung sei jedenfalls unbegründet.

49 Die Klägerin sei zu Unrecht der Ansicht, dass das Landgericht gegen die im Urteil des BGH vom 18.11.2024 aufgestellten Grundsätze verstoßen habe. Der BGH habe ausdrücklich betont, dass eine Verletzung einer datenschutzrechtlichen Norm noch keinesfalls dazu führe, dass ein Schaden in Form eines Kontrollverlustes über die Daten des Betroffenen vorliege. Vielmehr müsse ein solcher Kontrollverlust vom Anspruchsteller nachgewiesen werden. Es fehle vorliegend bereits an einer Darlegung der Klägerin, worin ein solcher Kontrollverlust bestanden habe. Die Behauptung, der Klägerin, dass neben den von der Beklagten beauftragten Dienstleistern weitere Dritte Zugriff auf personenbezogene Daten der Klägerin gehabt haben könnten, sei rein theoretischer Natur. Ein solcher Zugriff habe nicht stattgefunden.

50 Die geäußerte Ansicht der Klägerin, dass eine rechtswidrige Verarbeitung von Daten für einen Kontrollverlust ausreiche, lasse sich mit der höchstrichterlichen Rechtsprechung nicht in Einklang bringen. Voraussetzung sei vielmehr, dass personenbezogene Daten aufgrund einer Datenschutzverletzung Dritten zugänglich gemacht werden und es hierdurch zu einer missbräuchlichen Verwendung der personenbezogenen Daten durch den Dritten kommen kann. Dieses sei von der Klägerin jedoch nicht dargelegt worden. Der von der Beklagten beauftragte Dienstleister UNIwise ApS, mit dem die Beklagte einen Vertrag zur Auftragsdatenverarbeitung geschlossen habe, sei bereits kein Dritter im Sinne von Art. 4 Nr. 10 DSGVO. Die von der UNIwise ApS eingesetzten Dienstleister seien Unterauftragsverarbeiter gewesen und damit ebenso weisungsabhängig gewesen. Die Beklagte habe somit während der gesamten Dauer allein über die Zwecke und Mittel der Datenverarbeitung entscheiden können. Zudem habe die Klägerin zum Zeitpunkt der Prüfungen keine Kontrolle über ihre personenbezogenen Daten gehabt, da sie unstreitig seit 2015 in den sozialen Netzwerken aktiv gewesen sei und dort Fotos ihres Gesichts hochgeladen sowie Bewertungen über den Dienst GoogleMaps unter Verwendung ihres Klarnamens abgegeben habe. Soweit die Klägerin behaupte, dass sie ihr Instagramkonto inzwischen auf „privat“ gestellt habe, so sei dies über einen längeren Zeitraum nach den Onlineprüfungen noch nicht der Fall gewesen. Die Klägerin habe ihre personenbezoge-

nen Daten an in den USA ansässigen Konzerne zur Verfügung gestellt. Durch die Beklagte seien keine personenbezogenen Daten verarbeitet worden, die von der Klägerin nicht schon selbst ins Internet gestellt worden seien.

51 Das Landgericht habe zutreffend aufgrund der Anhörung der Klägerin festgestellt, dass die Frage der Rechtmäßigkeit der Datenverarbeitung für die Klägerin keine Rolle gespielt habe Soweit die Klägerin rüge, dass das Landgericht die erstinstanzlich vorgelegte Sprachnachricht nicht berücksichtigt habe, fehle es schon an Darlegungen, inwieweit deren Berücksichtigung zu einem anderen Ergebnis der Beweiswürdigung geführt hätte.

52 Im Übrigen sei die Datenverarbeitung durch die Beklagte rechtmäßig gewesen. Der Thüringer Landesbeauftragte für den Datenschutz und Informationsfreiheit sei nach Überprüfung zu dem Ergebnis gekommen, dass die Datenverarbeitung den Vorgaben entspreche.

53 Ein Verstoß gegen Art. 9 DSGVO liege nicht vor. Für die Verarbeitungstätigkeit habe eine Rechtsgrundlage bestanden. Zudem habe die Klägerin die hier in Rede stehenden Daten selbst der breiten Öffentlichkeit zur Verfügung gestellt. Aus den von ihr selbst veröffentlichten Lichtbildern seien biometrische Daten ableitbar, was bereits erstinstanzlich vorgetragen worden sei.

54 Ein Verstoß gegen Art. 22 DSGVO scheide aus, weil die Beurteilung der Prüfungsleistung gerade nicht ausschließlich auf einer automatisierten Entscheidung beruhe, da im Falle einer Unterschreitung des Referenzwerts die Aufsichtsperson gehalten sei, eine Entscheidung herbeizuführen. Das System biete lediglich eine Hilfestellung zur Vorbereitung für eine menschliche Entscheidungsfindung.

55 Auch ein Verstoß gegen Art. 44 DSGVO komme nicht in Betracht. Insoweit sei bereits erstinstanzlich dargelegt worden, dass keine Übermittlung von Daten in Drittstaaten erfolgt sei.

56 Zudem sei die von der Klägerin verlangte Schadenssumme deutlich übersetzt.

57 Mit Schriftsatz vom 24.09.2025 hat die Beklagte dargelegt, dass sich auch aus jüngeren Entscheidungen des EuGH und des BGH zu den Tatbestandsvoraussetzungen des Art. 82 Abs. 1 DSGVO ergebe, dass die Klägerin die Voraussetzungen eines Schadensersatzanspruchs nicht hinreichend dargelegt habe. So fehle es an Vortrag, dass es zur missbräuchlichen Verwendung personenbezogener Daten durch Dritte gekommen sei. Allein eine entsprechende Befürchtung der Klägerin reiche insoweit nicht aus. Die Auftrags- bzw. Unterauftragsdatenverarbeiter der Beklagten würden seien keine Dritten im Sinne des Art. 4 Nr. 10 DSGVO.

58 Das Landgericht habe zu Recht einen Schaden der Klägerin in Form einer psychischen Beeinträchtigung durch die Nutzung der Gesichtserkennungssoftware während der Online-Prüfungen verneint. Dass die Klägerin gerade durch die Verarbeitung biometrischer Daten in ihrem Wohlbefinden beeinträchtigt worden sei, sei somit nicht nachgewiesen worden.

II.

59 Die Berufung der Klägerin ist zulässig, insbesondere form- und fristgerecht eingelegt und begründet worden, §§ 517, 519, 520 ZPO. Entgegen der Auffassung der Beklagten ge-

nügt die Berufungsbegründung auch den Anforderungen des § 520 Abs. 3 Nr. 2 ZPO. Die Klägerin hat Umstände dargelegt, aus denen sich die Rechtsverletzung und deren Erheblichkeit für die angefochtene Entscheidung ergeben soll. Sie hat in der Begründung gerügt, dass das Landgericht in seinem Urteil zu Unrecht verneint habe, dass bereits ein Kontrollverlust über Daten einen ersatzfähigen Schaden darstelle und zudem eine immaterielle Beeinträchtigung der Klägerin durch die Nutzung der Gesichtserkennungssoftware bei den Online-Prüfung abgelehnt habe, in dem entgegen der europarechtlichen Rechtsprechung des EuGH faktisch eine gewisse Erheblichkeit der Beeinträchtigung für die Bejahung eines ersatzfähigen Schadens verlangt worden sei.

60 In der Sache hat das Rechtsmittel teilweise Erfolg.

61 Der Klägerin steht gemäß Art. 82 Abs. 1 DSGVO ein Anspruch auf Ersatz des ihr entstandenen immateriellen Schadens aufgrund der rechtswidrigen Verarbeitung biometrischer Daten der Kläger durch die Beklagte zu.

62 Bei der Nutzung der Gesichtserkennungssoftware des Anbieters Uniwise sind biometrische Daten der Klägerin im Sinne von Art. 4 Nr. 14 DSGVO verarbeitet worden. Durch den automatisierten Abgleich der während der Online-Prüfungen aufgenommenen Bilder vom Gesicht der Klägerin mit dem am 09.07.2020 erstellten Referenzbild wurden mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen der Klägerin, die ihre eindeutige Identifizierung ermöglichen oder bestätigen, zur Feststellung möglicher Täuschungsversuche verwendet. Diese Verarbeitung der biometrischen Daten der Klägerin war unter den hier vorliegenden Umständen auch rechtswidrig. Gemäß Art 9 Abs. 1 DSGVO ist die Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person grundsätzlich untersagt, es sei denn es liegt ein in Art. 9 Abs. 2 DSGVO geregelter Ausnahmefall vor. Ein solcher Ausnahmefall kann hier jedoch nicht angenommen werden.

63 Der in § 9 Abs. 2 Buchst. a DSGVO geregelte Fall einer ausdrücklichen Einwilligung der von der Verarbeitung ihrer biometrischen Daten betroffenen Person ist hier nicht gegeben. Eine solche ausdrückliche Einwilligung kann insbesondere nicht durch den Umstand angenommen werden, dass die Klägerin aus dem Katalog der möglichen Durchführung von Prüfungen während der Corona-Pandemie die Möglichkeit 1 (Absolvierung der Prüfung außerhalb des Unicampus) ausgewählt hat. In der Wahl dieser Prüfungsart liegt weder eine konkludente noch eine von der genannten Norm erforderte ausdrückliche Einwilligung der Klägerin mit der Verarbeitung ihrer biometrischen Daten. Der Umstand, dass nach der entsprechenden Auswahl durch die Klägerin ein Referenzbild von ihr angefertigt wurde, konnte zwar die Vermutung der Klägerin begründen, dass bei der Online-Prüfung eine automatisierte Gesichtserkennungssoftware zum Einsatz kommt. Durch die bloße Hinnahme dieses Procederes hat sie jedoch nicht ihr Einverständnis mit der konkreten Verarbeitung ihrer biometrischer Daten durch die zum Einsatz gebrachte Gesichtserkennungssoftware erklärt. Jedenfalls fehlt es insoweit an der im Gesetz vorgeschriebenen Ausdrücklichkeit der Einwilligungserklärung. Hierzu hätte es einer expliziten Belehrung der Klägerin über die durch die Nutzung der Gesichtserkennungssoftware ermöglichte Verarbeitung ihrer biometrischen Daten und einer hierauf bezogenen konkreten Einwilligungserklärung der Klägerin bedurft. Eine solche ausdrückliche Einwilligungserklärung hat sie nicht abgegeben. Auch die Möglichkeit, sich bei Auskunftsstellen der

Universität näher über den Prüfungsablauf informieren zu können, ersetzt das Erfordernis einer solchen ausdrücklichen Einwilligungserklärung nicht.

64 Die Zulässigkeit der Verarbeitung der biometrischen Daten der Klägerin ergibt sich auch nicht aus Art. 9 Abs. 2 Buchst. e DSGVO. Durch die Veröffentlichung von Gesichtsbildern in den sozialen Medien seit dem Jahr 2015 hat die Klägerin keine biometrischen Daten veröffentlicht, sondern lediglich die Möglichkeit geschaffen, dass Dritte biometrische Daten aus diesen Bildern gewinnen können. Ob die Klägerin durch die vorherige Veröffentlichung ihrer Bilder im Internet bereits die Kontrolle über diese personenbezogenen Daten verloren hat, spielt in diesem Zusammenhang keine Rolle, sondern ist erst für die Frage relevant, inwieweit ihr durch den Datenschutzverstoß ein Schaden entstanden ist.

65 Auch aus der Norm des Art. 9 Abs. 2 Buchst. g DSGVO kann keine Rechtfertigung für die Verarbeitung der biometrischen Daten hergeleitet werden. Zwar mag die Durchführung von Fernprüfungen während der Corona-Pandemie zwecks Aufrechterhaltung des Lehr- und Prüfungsbetriebes in den Hochschulen einem gewissen öffentlichen Interesse entsprochen haben. Dieses öffentliche Interesse erforderte es jedoch nicht wie geschehen eine Verarbeitung biometrischer Daten, durch die nicht unerheblich in das informationelle Selbstbestimmungsrecht des Betroffenen eingegriffen wird, ohne Einholung einer ausdrücklichen Einwilligungserklärung des Betroffenen vorzunehmen, zumal auch andere Möglichkeiten der Prüfungsdurchführung während der Pandemie zur Verfügung standen.

66 Durch die unzulässige Verarbeitung der biometrischen Daten der Klägerin bei der Durchführung der Online-Prüfungen ist dieser auch ein wenn auch eher als nicht allzu intensiv einzuschätzender Schaden in Form einer psychischen Beeinträchtigung entstanden, für den die Beklagte gemäß Art. 82 Abs. 1 DSGVO Ersatz zu leisten hat.

67 Die Klägerin hat bei ihrer Anhörung durch das Landgericht erklärt, dass sie während der Fernprüfungen aufgrund der Nutzung der Gesichtserkennungssoftware dauerhaft befürchtet habe, durch bestimmte Bewegungen ihres Kopfes den Übereinstimmungsreferenzwert zwischen aktuellem Bild und dem Referenzbild zu unterschreiten und hierdurch infolge der Softwarefunktion dem Prüfer automatisch Veranlassung zur Überprüfung eines Täuschungsversuches ihrerseits bieten könnte. Der Senat hält diese Bekundungen auch für plausibel. Insbesondere der Umstand, dass eine automatisierte Erkennungssoftware zum Einsatz gekommen ist, lässt das wenn auch vielleicht diffuse Gefühl, dass ohne eigene Einflussmöglichkeit ständig die Möglichkeit besteht, dem Vorwurf eines Täuschungsversuches ausgesetzt zu sein, durchaus nachvollziehbar erscheinen. Entgegen dem Vorbringen der Beklagten ist die Behauptung auch nicht deshalb unglaubhaft, weil sie erst im späteren Verlauf des Verfahrens aufgestellt wurde. Vielmehr hat die Klägerin bereits in der Klageschrift vorgetragen, dass die automatische Überwachung sie während der Prüfungssituation unter erheblichen Stress gesetzt habe und in ihr die Angst ausgelöst habe, dem unbegründeten Verdacht eines Täuschungsversuchs ausgesetzt zu sein. Dass das Landgericht diese Bekundung der Klägerin für unglaubhaft gehalten hat, ergibt sich aus den Ausführungen im Urteil nicht. Vielmehr meinte das Landgericht, hieraus nicht den Schluss ziehen zu können, dass der Klägerin ein immaterieller Schaden entstanden ist. Soweit das Landgericht damit argumentiert hat, dass der Umstand, dass sich die Klägerin vor den Prüfungen nicht bei Auskunftsstellen der Beklagten über den genauen Ablauf der Fernprüfungen informiert habe, gegen die Annahme eines immateriellen Schadens spreche, handelt es sich nach Auffassung des Senats letztlich um die unbewusste Anwendung des Erfordernisses einer Erheblichkeitsschwelle für die Annahme eines immateriellen Schadens durch das Landgericht, da dieses Argument nicht geeig-

net ist, die Befürchtungen der Klägerin als solche zu widerlegen, sondern die Annahme begründet, dass die Befürchtungen nicht allzu intensiv gewesen sein können. Die weitere Schlussfolgerung des Landgerichts, dass die psychische Beeinträchtigung nicht spezifisch auf die Verarbeitung biometrischer Daten zurückzuführen ist, da anzunehmen sei, dass diese auch bei der Durchführung herkömmlicher videoüberwachter Prüfungen aufgetreten sei, vermag der Senat nicht zu teilen. Zwischen diesen Prüfungssituationen besteht ein erheblicher Unterschied. Während bei einer bloß videoüberwachten Prüfung für den Prüfer nur dann Anlass besteht, Ermittlungen wegen eines möglichen Täuschungsversuchs aufzunehmen, wenn er durch eigene Anschauung entsprechende Anhaltspunkte hierfür gewonnen hat, wird die entsprechende Verdachtsprüfung durch den automatisierten Einsatz der Gesichtserkennungssoftware ausgelöst. Für den Prüfling besteht hierdurch ein Gefühl, „der Technik ausgeliefert zu sein“ und das Auslösen eines Verdachts der Täuschung letztlich nicht beeinflussen zu können. Die von der Klägerin geschilderten Befürchtungen sind also gerade auf die Verwendung der Gesichtserkennungssoftware und die hierdurch erfolgte Verarbeitung biometrischer Daten zurückzuführen.

68 Eine nochmalige Anhörung der Klägerin war entgegen der Auffassung der Beklagten nicht erforderlich, um bezüglich der Beweiswürdigung in Bezug auf den Eintritt einer psychischen Beeinträchtigung zu einem anderen Ergebnis zu kommen als das Landgericht. Die von derjenigen des Landgerichts abweichende Beweiswürdigung des Senats beruht nicht auf einer unterschiedlichen Einschätzung der Glaubhaftigkeit der Aussage der Klägerin, sondern auf divergierenden Schlussfolgerungen, die aus den Bekundungen der Klägerin im Hinblick auf den Eintritt eines ersatzfähigen Schadens gezogen wurden.

69 Der Senat bewertet den der Klägerin durch die erlittene psychische Beeinträchtigung entstandenen immateriellen Schaden mit einem Betrag von 200 EUR. Dabei war zu beachten, dass es sich nach Einschätzung durch den Senat vorliegend um eine eher geringfügige Beeinträchtigung von nicht sehr hoher Intensität handelt. Die Befürchtungen bestanden vorliegend nicht dauerhaft, wie das etwa bei der Veröffentlichung personenbezogener Daten im Internet der Fall ist, sondern nur punktuell während der Zeit der Fernprüfungen. Darüber hinaus drohten der Klägerin bei einem Auslösen des „Alarms“ durch die Software bei Unterschreitung des Referenzwertes noch keine unmittelbar nachteiligen Konsequenzen, sondern lediglich Maßnahmen zur Überprüfung des Grundes für das Auslösen der Software. Ein solche Überprüfung ist zwar für den Prüfling nachvollziehbarerweise mit unangenehmen Gefühlen verbunden, stellt aber noch kein so gravierendes Übel dar, dass von einer hohen psychischen Beeinträchtigung ausgegangen werden kann. Hinzu kommt, dass mit der Absolvierung mehrerer Fernprüfungen, bei denen der „Alarm“ durch die Software gerade nicht ausgelöst worden war, bei der Klägerin ein Gewöhnungseffekt eingetreten sein dürfte, der bei den später absolvierten Klausuren die Intensität der Befürchtungen, wenn sie überhaupt noch vorhanden waren, deutlich verringert haben dürfte. Der Senat hält daher die Bewertung des Schmerzensgeldbetrages mit einem im unteren Bereich der Bemessungsskala angesiedelten Betrag für gerechtfertigt.

70 Ein weitergehender Schaden in Form eines Kontrollverlustes über ihre biometrischen Schaden ist der Klägerin nicht entstanden. Allerdings hat der BGH in seiner nach Erlass des Urteils des Landgerichts ergangenen Leitentscheidung vom 18.11.2024, Az.:VI ZR 10/24, juris entschieden, dass der bloße Kontrollverlust über personenbezogene Daten bei dem von einem Datenschutzverstoß Betroffenen bereits einen ersatzfähigen Schaden darstellt. Jedoch muss der Betroffene den Eintritt eines solchen Kontrollverlusts dar-

legen und gegebenenfalls beweisen. Der Datenschutzverstoß als solcher stellt noch keinen Nachweis eines Kontrollverlusts dar.

71 Vorliegend hat die Klägerin durch die Verarbeitung ihrer biometrischen Daten schon deshalb keinen Kontrollverlust erlitten, weil sie zum Zeitpunkt der Datenverarbeitung bereits keine Kontrolle mehr über ihre ihr Gesicht betreffenden biometrischen Daten gehabt hat. Die Klägerin hat unstreitig Fotos von ihrem Gesicht seit 2015 auf stark besuchten Internetplattformen, insbesondere Instagram, veröffentlicht und erst 2022 die Sichtbarkeit dieser Bilder zumindest auf einen beschränkten Personenkreis reduziert. Damit bestand für eine unbegrenzte Vielzahl von Nutzern der Plattform Instagram über eine lange Zeitdauer die potentielle Möglichkeit, aus den Gesichtsfotos der Klägern biometrische Daten zu gewinnen. Dieses Vorbringen der Beklagten hat die Klägerin nicht bestritten. Die Generierung und Nutzung der biometrischen Daten der Klägerin war somit für eine unbegrenzte Vielzahl von Internetnutzern auf aller Welt gegeben, so dass die Klägerin nicht mehr die Kontrolle über ihre biometrischen Daten, soweit sie ihr Gesicht betreffen, besaß. Der Umstand, dass die Generierung und Nutzung von biometrischen Daten aus den von ihr veröffentlichten Bildern regelmäßig rechtswidrig sein dürfte, ändert am Eintritt des Kontrollverlusts nichts. Einem Kontrollverlust über personenbezogene Daten ist es gerade immanent, dass deren - insbesondere missbräuchliche - Verwendung durch Dritte durch den Betroffenen nicht mehr verhindert werden kann. Die Annahme der Klägerin, dass der von einem vor dem Datenschutzverstoß bereits eingetretenen Kontrollverlust Betroffene der Verwendung seiner Daten schutzlos ausgeliefert sei, ist unzutreffend. Selbstverständlich kann der Betroffene bei einer rechtswidrigen Generierung oder Verwendung seiner biometrischen (oder sonstigen personenbezogenen) Daten Schadensersatz geltend machen, wenn ihm hierdurch ein materieller oder immaterieller Schaden entstanden ist. Er kann lediglich keinen Schadensersatz wegen des (bloßen) Kontrollverlusts über seine personenbezogenen Daten mehr verlangen.

72 Schadensersatz wegen eines etwaigen Kontrollverlusts über ihre biometrischen Daten, der sich angesichts der Rechtsprechung des BGH im Urteil vom 18.11.2024, Az.: VI 10/24, wonach selbst der Kontrollverlust über dauerhaft im Darknet veröffentlichte personenbezogene Daten mit einem Schadensbetrag von etwa 100 EUR zu bewerten ist, ohnehin in einem eher symbolischen Bereich bewegen dürfte, kann die Klägerin somit nicht geltend machen.

73 Ein Verstoß gegen Art. 22 DSGVO liegt nicht vor. In dem Umstand, dass das Unterschreiten oder Nichtunterschreiten des Referenzwertes die Grundlage für eine Überprüfung des Vorliegens eines Täuschungsversuches bildet, sieht der Senat wie das Landgericht weder eine rechtliche wirksame Entscheidung für die Klägerin noch diese hierdurch „in ähnlicher Weise beeinträchtigt“. Das ist auch dann der Fall, wenn man wie angeblich in anderen Sprachversionen eine „beträchtliche Auswirkung“ fordert. Selbst wenn man einen Verstoß gegen Art. 22 DSGVO bejahen würde, stünde der Klägerin kein weitergehender Ersatz eines Schadens, den sie nicht bereits durch den Verstoß gegen Art. 9 Abs. 1 DSGVO verlangen kann, zu. Aus demselben Grund kann auch dahinstehen, ob dem Grunde nach Schadensersatzansprüche aus § 823 Abs. 2 BGB aus § 839 BGB i.V.m. Art. 34 GG oder aus § 25 TMMG gegeben sind.

74 Ein Verstoß gegen Art. 44 DSGVO (Übermittlung von Daten in Staaten außerhalb der EU) begründet ebenfalls keinen Schadensersatzanspruch, da eine entsprechende Datenschutzverletzung schon nicht feststeht. Insbesondere steht nicht fest, dass Daten an die in den USA ansässigen Gesellschaften der Mutterkonzerne Amazon bzw. Google übermit-

telt wurden. Darüber hinaus wäre die Klägerin durch die Übermittlung von Daten an den in den USA ansässigen Mutterkonzern Amazon aufgrund des bereits zuvor eingetretenen Kontrollverlust über ihre biometrischen Daten nicht zusätzlich geschädigt.

75 Ein Verstoß gegen die Verpflichtung der Beklagten, gemäß Art. 28 Abs. 3 und 4 DSGVO Verträge mit dem dort geregelten Inhalt mit den Auftrags- bzw. Unterauftragsverarbeitern zu schließen, dürfte zwar vorliegen, da die Beklagte solche Verträge trotz ausdrücklichen Bestreitens der Behauptung durch die Klägerin, dass solche existieren, nicht vorgelegt hat. Auch diesbezüglich hat die Klägerin jedoch keinen weitergehenden Schaden erlitten.

76 Auf die Geltendmachung von Schadensersatz wegen der Übermittlung von IP-Adressen der Klägerin an den Google-Konzern im Zusammenhang mit der Verwendung der Software WISEflow hat diese im Laufe des Verfahrens verzichtet. Die streitige Rechtsfrage (vgl. den Vorlagebeschluss des BGH an den EuGH vom 28.08.2025, Az.: VI ZR 258/24), in welchen Konstellationen an Dritte übermittelte IP-Adressen als personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO anzusehen sind, kann somit offenbleiben.

77 Die Klägerin kann ebenfalls keinen Schadensersatz wegen der Verwendung des Lock-Down-Browsers der Firma Respondus verlangen. Hierbei handelt es sich nicht um einen Datenschutzverstoß durch die Beklagte. Dass durch den Zugriff auf das seitens der Klägerin auf ihrem Laptop installierte Programm auf auf dem Endgerät gespeicherte Daten zugegriffen wurde, die über die Programmbibliotheken des Lock-Down-Programms selbst hinausgehen, hat die Klägerin weder substantiiert vorgetragen noch hierzu Beweis angetreten. Der Zugriff auf die Daten des Programms, welches die Klägerin selbst auf Veranlassung der Beklagten zur Verhinderung der Inanspruchnahme unerlaubter Hilfsmittel bei den Fernprüfungen installiert hat, ist nicht rechtswidrig. Die Klägerin hat sich durch die Installation des Programms zwecks Teilnahme an der Fernprüfung mit dem Zugriff auf die Programmdaten während der Prüfung zumindest konkludent einverstanden erklärt. Zudem ist nicht ersichtlich, dass die Klägerin durch den Zugriff auf die Programmbibliotheken des Lock-Down-Programms einen Schaden erlitten hat.

78 Die Klägerin hat gegen die Beklagte daher einen Anspruch auf Ersatz des ihr entstandenen immateriellen Schadens in Höhe von 200 EUR, so dass das Urteil des Landgerichts entsprechend abzuändern war.

79 Die Kostenentscheidung folgt aus §§ 92, 97 Abs. 1 ZPO.

80 Die Entscheidung über die vorläufige Vollstreckbarkeit des Urteils hat ihre Grundlage in §§ 708 Nr. 10, 713 ZPO.

81 Gründe für die Zulassung der Revision gemäß § 543 Abs. 2 ZPO sind nicht ersichtlich, nachdem die Rechtsfrage der Eigenschaft von an Dritte übermittelten IP-Adressen als personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO nicht mehr entscheidungserheblich ist.