Spirit Legal / Neumarkt 16-18 / 04109 Leipzig / Germany

Empfänger:
Landgericht Erfurt
Domplatz 37
99084 Erfurt

Übermittlung per beA

AZ: 21/806/ENK/PHE/CSC
Bearbeiter: Elisabeth Niekrenz
Ihr Zeichen:
Datum: 20.10.2022
Standort: Leipzig

Spirit Legal Fuhrmann Hense
Partnerschaft von Rechtsanwälten

Standort Leipzig:
Neumarkt 16-18
04109 Leipzig
Germany

Tel.: +49 (0) 341 / 39 29 78 90
Fax: +49 (0) 341 / 39 29 78 99

Standort Frankfurt am Main:
Bethmannstraße 58
60311 Frankfurt am Main
Germany

Tel.: +49 (0) 69 / 34 86 71 990
Fax: +49 (0) 69 / 34 86 71 999

Standort Dresden:
An der Herzogin Garten 1
01067 Dresden
Germany

Tel.: +49 (0) 351 / 21 78 88 00
Fax: +49 (0) 351 / 21 78 88 09

E-Mail: info@spiritlegal.com
Web: www.spiritlegal.com

AG Leipzig
Partnerschaftsregister No. 243

Klage

der **...**

- Klägerin -

Prozessbevollmächtigte: Spirit Legal Fuhrmann Hense Partnerschaft von Rechtsanwälten, Neumarkt 16 – 18, 04109 Leipzig

gegen

die **Universität Erfurt, KdÖR**, ges. vertr. d. d. Präsidenten Prof. Dr. Walter Bauer-Wabnegg, Nordhäuser Straße 63, 99089 Erfurt

- Beklagte -

Wegen: Allgemeines Persönlichkeitsrecht

Streitwert (vorläufig): 1.000,00 €

Namens und in Vollmacht der Klägerin erheben wir Klage und werden beantragen,

> ***die Beklagte zu verurteilen, an die Klägerin einen angemessenen Schadenersatz zu zahlen, dessen Höhe in das Ermessen des Gerichts gestellt wird, der mindestens jedoch EUR 1.000,00 (eintausend) beträgt.***

BEGRÜNDUNG

Die Klägerin verlangt von der Beklagten die Zahlung immateriellen Schadenersatzes nach Art. 82 DSGVO und § 839 Abs. 1 Satz 1 BGB i.V.m. Art. 34 Satz 1 GG aufgrund der rechtswidrigen Verarbeitung personenbezogener Daten der Klägerin im Rahmen der Durchführung und Überwachung elektronischer Fernprüfungen.

Diese Datenverarbeitungen verstießen gegen die Grundsätze für die Verarbeitung personenbezogener Daten aus Art. 5 DSGVO. Der Einsatz einer Gesichtserkennungssoftware war weder erforderlich noch verhältnismäßig und verstieß insbesondere gegen den Schutz, den biometrische Daten nach der DSGVO genießen (Art. 5 Abs. 1 lit. c) DSGVO, Art. 5 Abs. 1 lit. a) i.V.m. Art. 9 Abs. 1, 2 DSGVO). Rechtswidrig war auch die automatisierte Entscheidungsfindung durch die eingesetzte Software (Art. 22 DSGVO) sowie die Übermittlung von Daten in Drittstaaten (Art.44 ff. DSGVO). Schließlich verletzte die Beklagte das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sowie das TTDSG, in dem sie von der Klägerin verlangte, einen Lockdownbrowser auf ihrem privaten Rechner zu installieren.

Die Beklagte trägt aufgrund der in Art. 5 Abs. 2 DSGVO niedergelegten Rechenschaftspflicht als Verantwortliche die volle Darlegungs- und Beweislast hinsichtlich der Rechtmäßigkeit der von ihr durchgeführten Verarbeitung personenbezogener Daten der Klägerin [vgl. EuGH, Urt. v. 24. 02.2022 - C-175/20 - Rn. 77, 81; BVerwG, Urt. v. 02.03.2022 – 6 C 7.20, Rn. 49, dazu näher unter Pkt. B. II.2.].

Nachdem die Klägerin die Beklagte mit Schreiben vom 09.11.2021 zur Auskunft über die durch sie verarbeiteten personenbezogenen Daten nach Art. 15 DSGVO aufgefordert hatte, erteilte die

Beklagte diese Auskunft auch nach Aufforderung zur Nachbesserung nur unvollständig, sodass die Rechtmäßigkeit der Verarbeitung für die Klägerin nicht vollständig überprüfbar ist.

A. Zum Sachverhalt

I. Die Parteien

Die Beklagte ist eine staatliche Universität in Erfurt und als solche eine Körperschaft des öffentlichen Rechts.

Die Klägerin ist ehemalige Studentin bei der Beklagten. Von 2017 bis 2020 absolvierte sie ein Bachelorstudium mit dem Hauptfach *Primäre und Elementare Bildung*. Von 2020 bis 2022 studierte sie im *Master of Education Grundschule*. Im Rahmen dieses Studiums absolvierte sie elektronisch überwachte Fernprüfungen.

II. Abgelegte elektronische Fernprüfungen

Aufgrund der Kontaktbeschränkungen während der SARS-COV-2-Pandemie führte die Beklagte elektronische Fernprüfungen durch.

Die Beklagte setzte zur Durchführung der elektronischen Fernprüfungen die Software *WISEflow* des Anbieters *Uniwise ApS* (Jens Baggesens Vej 47, DK-8200 Aarhus N, Dänemark) ein.

WISEflow ist eine digitale Prüfungs- und Bewertungsplattform. Laut Angaben der Beklagten dient *WISEflow* der *„Vorbereitung, Durchführung, Bewertung und Archivierung von elektronischen Klausuren sowohl unter Aufsicht auf dem Campus als auch außerhalb des Campus als elektronische Fernprüfung mit automatisierter Überwachung (im Folgenden als „Proctoring“ bezeichnet)*“, der *„Abgabe, Plagiatsprüfung, Bewertung und Archivierung von schriftlichen Arbeiten;*“ sowie der *„Bereitstellung der Kopien der Prüfungsleistungen der Studierenden mit den Kommentierungen der Prüfenden*.“

Beweis: Auskunft der Beklagten vom 03.12.2021, S. 2,

vorgelegt als **Anlage K 1**

Unter Anwendung dieser Software nahm die Klägerin an den folgenden Fernprüfungen teil:

- „Fernklausur EKK 22.07.2021“ (22.07.2021)
- „[SoSe 2021] MEd Gr * Fö FDG Mat“ (20.07.2021)

- „Testklausur EKK 2021“ (16.07.2021)
- „Grundlagen Inklusiver Bildung“ (06.07.2021)
- „[SoSe 2021] MEd Gr * Fö FDG Mat * Test“ (29.06.2021)
- „Probeklausur Grundlagen inklusiver Bildung“ (18.06.2021)
- „Pädagogisch-psychologische Diagnostik“ (09.03.2022)
- „FinalExam_IntroTEFL“ (23.02.2021)
- „Klausur FD Deutsch 22.02.2021“ (22.02.2021)
- „2020WiSe Fachdidaktik Deutsch Probeklausur“ (01.02.2021)
- „MatG320 * PEB 325 * Klausur * SS2020 * 21.07.20“ (21.07.2020)
- „Testklausur3 * mit FLOWlock * Arithmetik“ (09.07.2020)

Beweis: Anlage zur Auskunft der Beklagten vom 24.03.2022: Datenübersicht zum Auskunftsverlangen 21/806/ENK/CSC, S. 84,

vorgelegt als **Anlage K 2**

III. Datenverarbeitung bei der elektronischen Überwachung von Fernprüfungen („Proctoring“)

1. Allgemeine Funktionsweise der eingesetzten Proctoring-Software

Bei dem eingesetzten Produkt *WISEflow* handelt es sich um eine cloudbasierte Software. Der Zugriff der Prüfungsteilnehmenden sowie der Lehrenden erfolgt über herkömmliche Webbrowser, wie z.B. Firefox oder Chrome. Die dabei erforderliche Datenverarbeitung findet auf den Servern des Anbieters *UNIwise ApS*. bzw. auf denen der von *UNIwise ApS.* eingesetzten Dienstleister statt. Prüfungsteilnehmenden und Lehrenden wird ein Account bereitgestellt, auf den sie mittels der jeweiligen Log-in-Informationen zugreifen können. Innerhalb des eigenen Accounts können Prüfungsteilnehmende unter anderem anstehende Prüfungen und absolvierte Prüfungen einsehen sowie an Prüfungen teilnehmen.

Beweis: Teilausdruck der Website der *UNIwise* ApS. vom 12.07.2022,

vorgelegt als **Anlage K 3**

Zur automatisierten Überwachung bzw. zur Verhinderung von Prüfungsbetrug umfasst *WISEflow* eine Funktion zur automatischen Gesichtserkennung der Prüfungsteilnehmenden, darunter der Klägerin. Diese wird über den in *WISEflow* integrierten Dienst *Amazon Rekognition* des Anbieters *Amazon Web Services EMEA S.à.r.l.* (38 Avenue John F. Kennedy, L-1855 Luxembourg) vorgenommen (dazu näher unter Ziffer III. 2.).

Darüber hinaus veranlasste die Beklagte die Installation des Programms *Lockdownbrowser* des Anbieters *Respondus, Inc.* (8201 164th Ave NE, Suite 200, Redmond, WA 98052, USA) auf dem Endgerät der Klägerin (dazu näher unter Ziffer III. 3.).

Schließlich veranlasste die Beklagte mittels *WISEflow* die Übermittlung von Daten betreffend die Klägerin in die USA (dazu näher unter Ziffer III. 4.).

Beweis: Schreiben der Beklagten vom 24.03.2022, S. 3,

vorgelegt als **Anlage K 4**

2. Automatische Gesichtserkennung

Am 09.07.2021 loggte sich die Klägerin im *WISEflow*-Portal ein. Es wurde über eine Kamera der Klägerin eine Fotografie des Gesichts der Klägerin (Referenzbild) angefertigt.

Beweis: Anlage zur Auskunft der Beklagten vom 03.12.2021: Bild-Protokoll Fernklausur EKK 22.07.2021,

vorgelegt als **Anlage K 5**

Ein Abgleich mit einem amtlichen Lichtbildausweis der Klägerin fand nicht statt.

Beweis: Schreiben der Beklagten vom 24.03.2022, S. 1f,

bereits vorgelegt als **Anlage K 4**

Beweis: Anleitung der Beklagten zur Durchführung von rechtssicheren und datenschutzkonformen elektronischen Prüfungen vom 14.09.2021, S. 1 f.,

vorgelegt als **Anlage K 6**

Anhand dieses Referenzbildes wurde das Gesicht der Klägerin, insbesondere das Verhältnis zwischen Augen, Nase, Stirn, Mund und anderen Gesichtsmerkmalen biometrisch vermessen. Das Gesicht der Klägerin wurde virtuell mit einer Umrisslinie umzeichnet; alles innerhalb dieser Linie wurde bei der Analyse berücksichtigt.

Beweis: Schreiben der Beklagten vom 24.03.2022, S. 1f,

bereits vorgelegt als **Anlage K 4**

Am 09.07.2021, am 21.07.2020, am 01.02.2021, am 23.02.2021, am 18.06.2021, am 29.06.2021, am 06.07.2021, am 22.07.2021, am 20.07.2021 und am 16.07.2021 nahm die Klägerin an elektronischen Fernklausuren unter Videoüberwachung teil.

Beweis: Anlage zur Auskunft der Beklagten vom 03.12.2021: Accountansicht_...,

vorgelegt als **Anlagen K 7**

Beweis: Bildprotokolle der einzelnen Prüfungen,

vorgelegt als **Anlagenkonvolut K 8**

Während dieser Prüfungen veranlasste die Software WISEflow, dass die Kamera des Endgeräts der Klägerin in unregelmäßigen Abständen Lichtbilder derselben (Verlaufsfotos) anfertigte. Auch anhand dieser Lichtbilder wurde das Gesicht der Klägerin biometrisch vermessen. Die entsprechenden Werte wurden „*mittels algorithmischen Abgleichs*“ mit den dem Referenzfoto entnommenen biometrischen Werten verglichen. Bei diesem Abgleich wurde ein Übereinstimmungswert der biometrischen Werte in Prozent ermittelt. Diese Übereinstimmungswerte sind und waren für die Prüfenden und weitere zur Einsicht berechtigte Personen einsehbar.

Liegt der Übereinstimmungswert unter 99 %, so *„ermittelt die/der Prüfende den konkreten Sachverhalt und kann erforderlichenfalls nach eigenem Ermessen die/den betreffende/n Studierenden, so auch Ihre Mandantin, um Erklärung zur möglichen Ursache für die Unterschreitung des o. g. Übereinstimmungswerts ersuchen. Sofern die Ursache seitens Ihrer Mandantin nicht nachvollziehbar begründet werden kann und aufgrund dessen der Verdacht einer Täuschungshandlung besteht, wird das hierfür vorgesehene Verfahren gemäß anwendbarer Studien- und Prüfungsordnung eingeleitet.“*

Beweis: Schreiben der Beklagten vom 24.03.2022, S. 1f,

bereits vorgelegt als **Anlage K 4**

3. Zugriff auf das Endgerät der Klägerin

a) Lockdownbrowser

Zur Durchführung der Prüfung

- „Testklausur3 * mit FLOWlock * Arithmetik“ (09.07.2020)

wurde die Klägerin von der Beklagten veranlasst, das Programm *Lockdownbrowser* des Anbieters *Respondus* (8201 164th Ave NE, Suite 200, Redmond, WA 98052, USA) auf dem eigenen Endgerät zu installieren und auszuführen. Diese Software erfüllte einerseits die klassischen Funktionen eines Webbrowsers, das heißt, sie ermöglichte den Abruf und die grafische Darstellung von Webseiten auf dem Bildschirm. Andererseits blockierte der Lockdownbrowser zum Zwecke der „Verhinderung von Prüfungsbetrug“ verschiedene Funktionen des Endgeräts der Klägerin, insbesondere das Aufrufen von anderen Internetverbindungen außer den für die jeweilige Prüfung erforderlichen, das Drucken sowie das Kopieren und Einfügen von Inhalten. Dazu speicherte das Programm Informationen auf dem Endgerät der Klägerin und las dort gespeicherte Informationen aus.

Beweis: Schreiben der Beklagten vom 24.03.2022, S. 5f,

bereits vorgelegt als **Anlage K 4**

b) Google Tag Manager

Während der o.g. Prüfungen, an denen die Klägerin teilgenommen hat, war auch der Dienst *Google Tag Manager* in *WISEflow* integriert. Dabei handelt es sich um ein System, dass die Einbindung verschiedener Elemente von Drittanbietern in ein Webangebot erleichtert. Bei Aufruf des *WISEflow*-Portals durch die Klägerin sendete ihr Browser aufgrund der Einbindung des *Google Tag Managers* unter Übermittlung ihrer IP-Adresse und weiterer Zugriffsdaten Serveranfragen an die *Google Ireland Ltd.* (Gordon House, Barrow Street, Dublin 4, Irland) sowie an die *Google, LLC* (1600 Amphitheatre Parkway Mountain View, CA 94043, USA).

Beweis: Teilausdruck der Website der Google Ireland Ltd, abrufbar unter: https://marketingplatform.google.com/intl/de/about/tag-manager/features/, abgerufen am 19.10.2022,

vorgelegt als **Anlage K 9**

Beweis: Teilausdruck der Website der Google Ireland Ltd, abrufbar unter: https://developers.google.com/tag-platform/tag-manager/server-side, abgerufen am 19.10.2022,

vorgelegt als **Anlage K 10**

4. Datentransfer in unsichere Drittländer

Die biometrische Gesichtserkennung wird durch den in *WISEflow* integrierten Dienst *Amazon Rekognition* durchgeführt. Vertragspartnerin der *UNIwise ApS.* ist diesbezüglich die *Amazon Web Services EMEA S.à.r.l.* (38 Avenue John F. Kennedy, L-1855 Luxembourg). Standort der Server, auf denen die Datenverarbeitung durchgeführt wird, ist laut Angaben der Beklagten Irland.

Beweis: Schreiben der Beklagten vom 24.03.2022, S. 3,

bereits vorgelegt als **Anlage K 4**

Die *Amazon Web Services EMEA SARL* ist eine Tochtergesellschaft der *Amazon Web Services, Inc.*

(410 Terry Avenue North, Seattle, WA 98109-5210, USA).

Amazon Rekognition ist eine cloudbasierte Software der *Amazon Web Services, Inc*. Bei der dahinterliegenden Technologie handelt es sich um sogenanntes „maschinelles Lernen“. Die Leistung der Technologie fußt insbesondere auf der Vielzahl der eingespeisten Trainingsdaten. Auch wenn der Dienst über eine in Europa ansässige Tochtergesellschaft der *Amazon Web Services, Inc.* vertrieben wird, erfolgt die Datenverarbeitung auch für europäische Kunden in den USA. Zumindest werden für den Betrieb von *Amazon Rekognition* Ressourcen der Domänen von AWS in den USA geladen.

Wie unter Pkt. A III. 3. b) dargelegt, übermittelte die Beklagte personenbezogene Daten der Klägerin aufgrund der Einbindung des *Google Tag Managers* Serveranfragen an die *Google Ireland Ltd.* (Gordon House, Barrow Street, Dublin 4, Irland) sowie an die *Google, LLC* (1600 Amphitheatre Parkway Mountain View, CA 94043, USA).

Zudem wurden personenbezogene Daten der Klägerin, nämlich ihr zugewiesene IDs, an die *Functional Services, Inc.* (45 Fremont Street, 8th Floor, San Francisco, CA 94105, US), an die *Zendesk, Inc.* (989 Market Street, San Francisco, CA 94103, USA) sowie an die *Z3CH.com LLC* (12 S. Main St. #412, Allentown, NJ 08501, US) übermittelt.

Beweis: von der Beklagten an die Klägerin übermittelte Aufstellung: WISEflow Sub-processors,

vorgelegt als **Anlage K 11**

Erst am 15.12.2021 schloss die Beklagte mit der *UNIwise ApS* die gesetzlich verpflichtenden Standarddatenschutzklauseln der EU-Kommission ab.

Beweis: Standard Contractual Clauses, Data Processing Agreement WISEflow/Universität Erfurt vom 15.12.2021, S. 11,

vorgelegt als **Anlage K 12**

5. Kenntnis der Datenverarbeitungen

Wie aus den Datenschutzinformationen der Beklagten über den Einsatz von WISEflow hervorgeht, wussten deren Entscheidungsträger um die unter Ziffer III. 1. – 4. vorgetragenen Umstände der Datenverarbeitung.

Beweis: Datenschutzerklärung der Beklagten zur Nutzung von Wiseflow, Stand: März 2022,

vorgelegt als **Anlage K 13**

6. Schaden der Klägerin

Die Klägerin erlitt und erleidet durch die Datenverarbeitungen der Beklagten einen empfindlichen und irreversiblen Schaden.

[1] Die Klägerin erlitt einen Verlust der Kontrolle über ihre hochsensiblen biometrischen Daten. Biometrische Daten werden zum Teil zur Identifizierung von Personen eingesetzt, z.B. bei amtlichen Ausweisdokumenten oder zur Entsperrung von Mobiltelefonen. Gelangen diese Daten in die Hände von Unbefugten, so geht von ihnen ein enormes Missbrauchspotenzial aus. Sie können zum Identitätsdiebstahl verwendet werden. Dies wiegt umso schwerer, als Betroffene – wie die Klägerin – die Biometrie ihres Gesichts anders als ein Passwort oder eine Telefonnummer niemals ändern können, wenn Informationen darüber verloren gehen. Vor dem Hintergrund, dass die luxemburgische Datenschutzaufsichtsbehörde CNDP im Juli 2021 wegen Datenschutzverstößen ein Bußgeld in Höhe von 756 Mio. Euro gegen die *Amazon Europe Core S.à.r.l.* verhängte [vgl. ZD-Aktuell 2021, 05315], muss die Klägerin befürchten, dass ihre mittels Amazon Rekognition verarbeiteten biometrischen Daten von Gesellschaften des Amazon-Konzerns zu eigenen Zwecken aufbewahrt, weiterverarbeitet und an Dritte weitergegeben werden. Zudem birgt jede Verarbeitung von Daten das Risiko des Abhandenkommens derselben in sich, etwa durch Hackerangriffe.

[2] Die automatische Überwachung setzte die Klägerin in den Prüfungssituationen zudem unter erheblichen Stress und löste in ihr die Angst aus, den (unbegründeten) Verdacht von Betrugsversuchen zu erwecken.

[3] Aufgrund der Übermittlung der IP-Adresse an Dritte wie die *Google Ltd.* sowie die *Google LLC*, Unternehmen, die bekanntermaßen Daten über Internetnutzende sammeln und zu

verschiedensten Zwecken verwerten, erlitt die Klägerin einen Verlust über die Kontrolle ihrer Daten. Bekanntermaßen sammeln die Unternehmen des Google-Konzerns Daten über ihre Nutzer und verwenden diese zu eigenen Zwecken [vgl. LG München I, Urt. v. 20.01.2022 – 3 O 17493/20, Rn. 12].

[4] Im Hinblick auf die Installation des Lockdownbrowsers erlitt die Klägerin eine Einschränkung der Nutzbarkeit ihres Endgeräts, verbunden mit dem Verlust des Vertrauens in den Schutz der dort gespeicherten Informationen. Mit der Installation des Lockdownbrowsers gehen erhebliche Gefahren für die IT-Sicherheit des Endgeräts der Klägerin einher. Zu diesem Ergebnis kommt ein Gutachten des Diplom-Informatikers und IT-Sicherheits-Experten Mike Kuketz. Das Gutachten befasst sich näher mit dem Browser-Add-on Proctorio, enthält jedoch auch allgemeine Aussagen über die Gefahren von Proctoring-Software. Speziell zu Standalone Software (wie dem *Lockdownbrowser* des Anbieters *Respondus, Inc.*) heißt es in dem Gutachten:

„Im Gegensatz zu Browser-Add-ons wird eine Standalone Software als zusätzliche Anwendung auf einem Betriebssystem installiert.

*Während Browser-Add-ons je nach Berechtigungen schon eine beachtliche Menge an Informationen über die Nutzer*innen und ihre Daten abfragen können, geht von Standalone Software eine ungleich höhere Gefahr aus. Ausgehend von einem Standard-Windows-System, bei dem in der Regel mit Admin-Rechten gearbeitet wird, ist eine Proctoring-Software nach der Installation grundsätzlich zu (fast) allem in der Lage. Ein Browser ist aus guten Gründen so konzipiert, einer Website keinen Vollzugriff auf das Betriebssystem und die auf dem System befindlichen Daten zu gewähren. Alles läuft in der Regel in einer geschützten Sandbox, also einem isolierten Bereich, der den Browser und die darin befindlichen Add-ons vom System abschottet.*

Eine Proctoring-Software umgeht diese für Browser-Add-ons eingezogene Brandmauer, verändert das darunter liegende Betriebssystem und lässt im ungünstigen Fall, konkret durch unsaubere De-Installationsroutinen, ein unsicheres System zurück.

In diesem Kontext wäre es vermutlich einfacher zu fragen: Auf welche Informationen hätte eine Proctoring- Software (je nach Betriebssystem und Rechteverwaltung) keinen Zugriff?“

[Spähsoftware gegen Studierende – Online-Proctoring als Gefahr für die IT-Sicherheit und den Datenschutz, IT-Gutachten vom 14.07.2021, https://freiheitsrechte.org/home/wp-content/uploads/2021/07/GFF_IT-Gutachten_Proctoring-Spaehsoftware-gegen-Studierende.pdf,

abgerufen am 15.10.2022]

Dass die Gefahren von Proctoring-Software real sind, zeigt das Beispiel Proctorio. Hier wurde 2021 eine Sicherheitslücke entdeckt, die sogenannte Universal Cross-Site Scripting-Angriffe ermöglichte. Angreifende konnten unter Umständen sogar ohne Kenntnis und Einwilligung der Betroffenen die Kamera aktivieren [Sector 7, Proctorio Chrome extension Universal Cross-Site Scripting, 14.12.2021, https://sector7.computest.nl/post/2021-12-proctorio/, abgerufen am 16.10.2022].

IV. Erfolglose Fristsetzung

Die Klägerin legte der Beklagten die Rechtsverletzungen in einem Schreiben vom 24.05.2022 ausführlich dar und forderte sie unter Fristsetzung zum 07.06.2022, auf Bitten der Beklagten verlängert bis zum 29.06.2022, auf, Schadenersatz zu leisten.

Beweis: Aufforderungsschreiben der Klägerin vom 24.05.2022,

vorgelegt als **Anlage K 14**

Die Beklagte leistete keinen Schadensersatz, sodass Klage geboten ist.

B. Rechtliche Würdigung

Der mit der zulässigen Klage geltend gemachte Anspruch ist begründet.

I. Zulässigkeit

Die Klage ist zulässig. Für die Klage steht der Rechtsweg zu den ordentlichen Gerichten offen. Materiell handelt es sich bei dem Schadenersatzanspruch aus Art. 82 DSGVO gegenüber staatlichen Stellen um einen Anspruch aus der Verletzung öffentlich-rechtlicher Pflichten. Hierfür ist nach § 40 Abs. 2 Satz 1 VwGO der Rechtsweg zu den ordentlichen Gerichten gegeben [Hessisches LSG, Beschluss vom 26.01.2022 – L 6 SF 7/21 DS]. Für den Schadensersatzanspruch aus § 839 Abs. 1 Satz 1 BGB i.V.m. Art. 34 Satz 1 GG ergibt sich der ordentliche Rechtsweg ebenfalls aus § 40 Abs. 2

Satz 1 VwGO.

Die Zuständigkeit des LG Erfurt ergibt sich aus § 71 Abs. 2 Nr. 2 GVG und aus § 71 Abs. 3 GVG i. V. m. § 6 Nr. 1 ThürAGGVG.

II. Begründetheit

Die Klage ist begründet. Die Klägerin hat einen Anspruch auf Zahlung von Schadensersatz in Höhe von 1.000 € aus Art. 82 Abs. 1 DSGVO (dazu unter Ziffer 1.) und aus § 839 Abs. 1 Satz 1 BGB i.V.m. Art. 34 Satz 1 GG (dazu unter Ziffer 2.).

1. Anspruch aus Art. 82 DSGVO

Anspruchsvoraussetzung des Schadenersatzanspruchs nach Art. 82 DSGVO ist ein „Verstoß gegen die Verordnung“. Darunter ist jede Verletzung materieller oder formeller Bestimmungen der Verordnung zu verstehen [OLG Stuttgart, Urt. v. 31.03. 2021 – 9 U 34/21, BeckRS 2021, 6282 Rn. 25; Quaas, in: Wolff/Brink, BeckOK Datenschutzrecht, Stand 01.11.2020, Art. 82 Rn. 14; Kohn, ZD 2019, 498, 500]. Von dem weiten Begriff sind auch Verstöße gegen die allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten aus Art. 5 DSGVO wie auch die Verletzung von Betroffenenrechten der Art. 12 ff. DSGVO umfasst, ohne dass es auf einen Schutznormcharakter der Vorschrift ankäme [OLG Stuttgart, Urt. v. 31.03. 2021 – 9 U 34/21, BeckRS 2021, 6282 Rn. 25; Kohn, ZD 2019, 498, 500].

Da die Klägerin keinerlei Einblick in die Verarbeitungsprozesse der Beklagten hat, trägt die Beklagte die volle Beweislast für die Einhaltung der Vorschriften der DSGVO.

Der Europäische Gerichtshof hat mit Urteil vom 24.02.2022 [C-175/20 – Valsts ieņēmumu dienests = ZD 2022, 271 ff.] klargestellt, dass die Beweislast für die Einhaltung der DSGVO vollständig beim Verantwortlichen liegt, hier also bei der Beklagten:

> *„(77) In diesem Zusammenhang ist darauf hinzuweisen, dass der für die Verarbeitung Verantwortliche nach dem in Art. 5 Abs. 2 der Verordnung 2016/679 verankerten Grundsatz der Rechenschaftspflicht nachweisen können muss, dass er die in Abs. 1 dieses Artikels festgelegten Grundsätze für die Verarbeitung personenbezogener Daten einhält.*
>
> *(…)*

(81) Wie sich oben aus Rn. 77 ergibt, obliegt die Beweislast insoweit der lettischen Steuerverwaltung."

Die Entscheidung des EuGH wurde bereits wenige Tage später in der höchstrichterlichen deutschen Rechtsprechung rezipiert, das Bundesverwaltungsgericht entschied [Urteil vom 02.03.2022, BVerwG 6 C 7.20, Rn. 50]:

„[…] Nach dieser Rechtsprechung enthält Art. 5 Abs. 2 DSGVO mithin eine Beweislastregelung für Streitigkeiten, in denen die Einhaltung der Grundsätze der Datenverarbeitung nach Art. 5 Abs. 1 DSGVO in Frage steht.[…]"

Auch im Schrifttum wurde das Urteil des EuGH begrüßt [Zerdick, EuZW 2022, 527, 533]:

„[…] Gleichzeitig bekräftigt der EuGH in zu begrüßender Weise, dass der in Art. 5 II DS-GVO neu verankerte und zentrale Grundsatz der datenschutzrechtlichen Rechenschaftspflicht des Verantwortlichen vollumfänglich für den öffentlichen Bereich gilt (Rn. 77). Die Rechenschaftspflicht geht insoweit einher mit einer Beweislast des Verantwortlichen (Rn. 81). Damit erteilt der EuGH einer im deutschen Schrifttum vertretenen „engen Auslegung" der Rechenschaftspflicht (s. zum Meinungsstand Jaspers/Schwartmann/Thüsing/Kugelmann, DS-GVO/BDSG/Herman, 2. Aufl. 2020, Art. 5 Rn. 80 mwN) eine klare Absage. […]"

Die Entscheidung des EuGH bringt Klarheit für die Beweislast bei komplexen Sachverhalten vor Gericht [Hense, ZD 2022, 413, 414]:

„[…] Eine europarechtliche Beweislastumkehr ist „nihil sub sole novi", nichts Neues unter der Sonne des Prozessrechts und demnach auch kein Grund zur Aufregung, sondern ein freundlicher Appell an die Verantwortlichen komplexer Datenverarbeitungsvorgänge, ihre Dokumentation in den Griff zu bekommen, wenn sie nicht vor Gericht Schiffbruch erleiden wollen. […]"

Demnach trägt die Beklagte die volle Beweislast für die Rechtmäßigkeit ihrer Datenverarbeitung. Außergerichtlich ist die Beklagte dieser Verpflichtung zum Nachweis der Rechtmäßigkeit nicht nachgekommen. Die erteilten Auskünfte sind auch nach mehreren Anläufen noch lückenhaft aber die übermittelten Informationen lassen bereits auf erhebliche Rechtsverstöße schließen. Im Einzelnen:

a) Verstoß gegen Art. 5 Abs. 1 lit. c) DSGVO

Die Durchführung von Video-Proctoring mittels biometrischer Gesichtserkennung ist zur Erfüllung ihres Zweckes weder geeignet noch erforderlich. Der angegebene Zweck „*Identifizierung der Prüfungsteilnehmenden bei Fernprüfungen durch die Kombination von personengebundenem Login und (unveränderlichem) Referenzfoto*“ kann nicht erfüllt werden, da eine Überprüfung des Referenzbildes mit einem amtlichen Lichtbildausweis nicht stattfindet, sodass nicht sichergestellt ist, dass es sich bei der auf dem Referenzbild abgebildeten Person tatsächlich um die Klägerin handelt. Auch widerspricht der Einsatz biometrischer Gesichtserkennung dem Grundsatz der Datenminimierung, Art 5 Abs. 1 lit. c) DSGVO, da die Nutzung einer derart invasiven Technologie zur Identifizierung der Prüfungsteilnehmenden nicht erforderlich ist. Die Identifizierung könnte zuverlässiger und weit weniger eingriffsintensiv durch eine Aufsichtsperson, die mittels einer Videokonferenz die Prüfungsteilnehmenden beaufsichtigt und zu Beginn der Prüfung einen Abgleich mit einem amtlichen Lichtbildausweis vornimmt, stattfinden. Die bloße Übertragung ist ausreichend, um Täuschungen zu verhindern. Sie ist das funktionale Äquivalent zur Aufsicht bei der Präsenzprüfung und als solche geeignet, das durch die Online-Prüfung erhöhte Täuschungspotenzial auszugleichen [vgl. Albrecht/Mc Grath/Uphues, ZD 2021, 80, 81, 84].

b) Verstoß gegen Art. 9 Abs. 1 DSGVO

Die Verarbeitung biometrischer Daten der Klägerin ist rechtswidrig, Art. 9 Abs. 1, 2 DSGVO.

Biometrische Daten sind personenbezogene Daten besonderer Kategorien nach Art. 9 Abs. 1 DSGVO, deren Verarbeitung grundsätzlich untersagt ist. Ausnahmen von diesem Verbot sind in Art. 9 Abs. 2 DSGVO geregelt.

Ausweislich der *Datenschutzerklärung über die Nutzung von WISEflow an der Universität Erfurt* (bereits vorgelegt als **Anlage K 13**, S. 2) stützt die Beklagte die Verarbeitung biometrischer Daten auf Art. 9 Abs. 2 lit. g) DSGVO i.V.m. § 11 Abs. 1 S. 1 ThürHG. Demnach dürfen Hochschulen personenbezogene Daten verarbeiten, soweit dies unter anderem für die Durchführung von Prüfungen in elektronischer Form erforderlich ist.

[1] Wie unter Pkt. B. II. 1. a) dargelegt, ist der Einsatz von Gesichtserkennungssoftware zur Durchführung elektronischer Prüfungen nicht erforderlich.

[2] § 11 Abs. 1 S. 1 Thüringer Hochschulgesetz (ThürHG) ist keine Erlaubnisnorm i. S.d. Art. 9 Abs. 2 lit. g) DSGVO.

Art. 9 Abs. 2 lit. g) DSGVO erlaubt die Verarbeitung personenbezogener Daten besonderer Kategorien, wenn die Verarbeitung

- *„auf Grundlage des Unionsrechts oder des Rechts eines Mitgliedsstaats,*
- *dass in angemessenem Verhältnis zu dem verfolgten Ziel steht,*
- *den Wesensgehalt des Rechts auf Datenschutz wahrt und*
- *angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht,*
- *aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist.“*

§ 11 Abs. 1 S. 1 Thüringer Hochschulgesetz (ThürHG) entspricht diesen Anforderungen nicht.

Art. 9 Abs. 2 lit. g) DSGVO soll insbesondere den Bereich der öffentlichen Sicherheit und der Gefahrenabwehr betreffen und für besondere Ausnahmesituationen gelten, wobei an die Zulässigkeit der Verarbeitung strenge Anforderungen zu stellen sind [Mester, in: Taeger/Gabel, DSGVO – BDSG – TTDSG, 4. Aufl. 2022, Art. 9 Rn. 28]. § 11 Abs. 1 Nr. 1 ThürHG stellt keine Anforderungen an die Verhältnismäßigkeit der Datenverarbeitung. Es sind keine Vorkehrungen zur Wahrung der Grundrechte und Interessen der betroffenen Personen oder des Wesensgehalts des Rechts auf Datenschutz vorgesehen. Die Verarbeitung biometrischer Daten wird durch das ThürHG weder ausdrücklich gestattet, noch ist sie zur Wahrung eines erheblichen öffentlichen Interesses erforderlich.

[3] Dass die Verarbeitung biometrischer Daten im Rahmen von elektronischen Prüfungen nicht mit der DSGVO vereinbar ist, zeigen auch aktuelle aufsichtsbehördliche Publikationen und Entscheidungen.

So stellt der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Nordrhein-Westphalen in der *Handreichung zu Online-Prüfungen an Hochschulen* fest:

„Die Verarbeitung biometrischer Daten ist unzulässig. Dies entspricht nicht der Vergleichssituation einer Präsenzklausur. Ein Abgleich mit einem gültigen Lichtbildausweis vor der Kamera ohne Einsatz einer solchen Software reicht aus“ [*Handreichung zu Online-Prüfungen an Hochschulen* des Landesbeauftragen für Datenschutz und Informationsfreiheit Nordrhein-Westphalen vom

28.07.2022, https://www.ldi.nrw.de/handreichung-zu-online-pruefungen-hochschulen, abgerufen am 15.08.2022, Hervorhebungen durch die Unterzeichnenden].

In einer Handreichung des Landesbeauftragten für den Datenschutz Niedersachsen heißt es:

„Der Einsatz besonderer Überwachungsprogramme, die biometrische Daten verarbeiten, ist mangels einer spezialgesetzlichen Rechtsgrundlage unzulässig und wäre auch stets als unverhältnismäßig anzusehen“ [Eckpunkte für die datenschutzkonforme Durchführung von Online-Prüfungen in den niedersächsischen Hochschulen (Stand: November 2021), https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/eckpunkte-fur-datenschutzkonforme-online-prufungen-an-niedersachsischen-hochschulen-206497.html, abgerufen am 15.10.2022]

Die italienische Datenschutzbehörde (Garante per la protezione dei dati personali – GPDP) erkannte im Einsatz eines Proctoring-Systems mit Gesichtserkennung durch die Wirtschaftsuniversität *Luigi Bocconi* in Mailand zutreffend einen Verstoß gegen Art. 9 DSGVO und verhängte eine Geldbuße in Höhe von 200.000,00 Euro [Etteldorf, ZD-Aktuell 2021, 05507].

Auch die französische Datenschutzbehörde (Commission Nationale de l’Informatique et des Libertés – CNIL) hält Gesichtserkennung bei Online-Prüfungen für unverhältnismäßig [Surveillance des examens en ligne: les rappels et conseils de la CNIL, 20.05.2022, https://www.cnil.fr/fr/surveillance-des-examens-en-ligne-les-rappels-et-conseils-de-la-cnil, abgerufen am 15.10.2022].

c) Verstoß gegen Art. 22 DSGVO

Im Rahmen der Prüfungsüberwachung mittels biometrischer Gesichtserkennung findet eine automatisierte Entscheidungsfindung statt. Bereits die automatisierte Einordnung und Kennzeichnung („Flagging“) eines Prüfungsverlaufs als verdächtig stellt eine auf einer automatisierten Verarbeitung beruhende Entscheidung im Sinne des Art. 22 Abs. 1 DSGVO dar, die die Betroffenen erheblich beeinträchtigt [vgl. zu solchen „Anomaly Detection-Systemen“: Binns, Veale: Is that your final decision?, International Data Privacy Law 2021, Volume 11, Issue 4, November 2021, Pages 319–332]. In der vorliegenden Gestaltung führt das Flagging eines Prüfungsverlaufs als verdächtig dazu, dass die Betroffenen selbst nachvollziehbar begründen müssen, weshalb die automatisierte Überprüfung eine Unterschreitung des

Übereinstimmungswerts zwischen Referenzfoto und Verlaufsfoto ergeben hat, obgleich dies den Betroffenen mangels Einblicks in die technische Funktionsweise regelmäßig nicht möglich ist. So heißt es auf S. 2 des Schreibens der Beklagten vom 24.03.2022 [bereits vorgelegt als **Anlage K4**]: Liege der Übereinstimmungswert unter 99 %, so „*ermittelt die/der Prüfende den konkreten Sachverhalt und kann erforderlichenfalls nach eigenem Ermessen die/den betreffende/n Studierenden, so auch Ihre Mandantin, um Erklärung zur möglichen Ursache für die Unterschreitung des o. g. Übereinstimmungswerts ersuchen. Sofern die Ursache seitens Ihrer Mandantin nicht nachvollziehbar begründet werden kann und aufgrund dessen der Verdacht einer Täuschungshandlung besteht, wird das hierfür vorgesehene Verfahren gemäß anwendbarer Studien- und Prüfungsordnung eingeleitet.*“.

Dass vor Einleitung des entsprechenden Verfahrens zum Prüfungsausschluss eine menschliche Beteiligung stattfindet, steht der Anwendung des Art. 22 DSGVO nicht entgegen, wie die portugiesische Datenschutzaufsichtsbehörde CNPD zum Einsatz der Proctoring-Software des Anbieters *Respondus, Inc*. entschied [vgl. die Entscheidung der portugiesischen Datenschutzaufsichtsbehörde CNPD - Deliberação/2021/622].

Die Anforderungen des Art. 22 Abs. 1, 2 und 4 DSGVO an die automatisierte Entscheidungsfindung, die im Rahmen des Video-Proctoring stattfindet, werden nicht gewahrt. Insbesondere liegt weder die Einwilligung der Klägerin in die Verarbeitung biometrischer Daten vor, noch stellt § 11 Abs. 1 Nr. 1 ThürHG eine den Anforderungen des Art. 9 Abs. 1 lit. g) DSGVO an die erforderliche Grundlage im Recht der Mitgliedstaaten genügende Rechtsgrundlage dar [vgl. Pkt. B. II. b) (ii)].

d) Verstoß gegen die Art. 44 ff. DSGVO

Die Transfers personenbezogener Daten der Klägerin an Anbieter mit Sitz in Ländern außerhalb der Europäischen Union, namentlich Amazon Web Services, Inc., Functional Software, Inc. [Sentry.io), Zendesk, Inc. und T3CH.com LLC (status.io) verstoßen gegen die Art. 44 ff. DSGVO. Standarddatenschutzklauseln im Sinne von Art. 46 Abs. 2 lit. c) DSGVO wurden erst am 15.12.2021 mit Uniwise ApS vereinbart, für die vor diesem Zeitpunkt stattfindenden Datentransfers ist keinerlei Rechtfertigung nach den Art. 44 ff. DSGVO ersichtlich.

e) Verstoß gegen Art. 6 Abs. 1 lit. a) DSGVO i. V. m. § 25 Abs. 1 Satz 2 TTDSG

Die Verarbeitung erfolgt unter Verstoß gegen § 25 Abs. 1 Satz 2 TTDSG.

Bei der Sperrung des Endgeräts der Klägerin durch den Lockdownbrowser wurden Informationen in ihrer Endeinrichtung gespeichert. Durch die Einbindung des Google Tag Managers fand ein Zugriff auf in ihrem Endgerät gespeicherte Informationen statt. Beides ist gemäß § 25 Abs. 1 S. 2 TTDSG i.V.m. Art. 6 Abs. 1 S. 1 lit. a) DSGVO nur auf Grundlage einer Einwilligung der Klägerin zulässig. Diese hat sie nicht erteilt. Die Ausnahmen vom Einwilligungserfordernis nach § 25 Abs. 2 TTDSG sind ersichtlich nicht einschlägig.

Der Verstoß gegen § 25 TTDSG zieht die Rechtsfolgen des Art. 82 DSGVO nach sich: § 25 TTDSG setzt die Anforderungen der ePrivacy-Richtlinie (RL EG 2002/58/EG), insbesondere des Art. 5 Abs. 3, in nationales Recht um. Gemäß Art. 15 Abs. 2 ePrivacy-Richtlinie ist bei Verstößen gegen nationale Normen, die die Richtlinie umsetzen, das Haftungs- und Sanktionsregime der DSGVO anwendbar. Konkret bezeichnet ist die bei Erlass der Richtlinie bezeichnete Vorgängernorm der DSGVO, die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr:

„Die Bestimmungen des Kapitels III der Richtlinie 95/46/ EG über Rechtsbehelfe, Haftung und Sanktionen gelten im Hinblick auf innerstaatliche Vorschriften, die nach der vorliegenden Richtlinie erlassen werden, und im Hinblick auf die aus dieser Richtlinie resultierenden individuellen Rechte."

Gemäß Art. 94 Abs. 2 Satz 1 DSGVO gilt dieser Verweis auf die Richtlinie 95/46/EG als Verweis auf die DSGVO.

Dies bestätigt auch der Zusammenschluss der europäischen Datenschutzaufsichtsbehörden (Europäischer Datenschutzausschuss, EDSA, im Englischen: European Data Protection Board, EDPB) in seiner Stellungnahme zum Verhältnis zwischen DSGVO und ePrivacy-Richtlinie [Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, task and powers of data protection authorities, 12.03.2019, Rn. 62]:

„The ePrivacy Directive particularises and complements the GDPR and moreover refers to the latter's provisions on judicial remedies, liability and sanctions (article 15(2) of the ePrivacy Directive read in light of article 94 of the GDPR).“

f) Schaden

Der immaterielle Schaden ist im Rahmen einer unionsautonomen Auslegung der DSGVO und

insbesondere Art. 82 DSGVO festzustellen. Zum Schadensbegriff heißt es in ErwG 146 explizit:

„*Der Begriff des Schadens sollte im Lichte der Rechtsprechung des Gerichtshofs weit auf eine Art und Weise ausgelegt werden, die den Zielen dieser Verordnung in vollem Umfang entspricht.*“

Konkrete Beispiele für einen materiellen oder immateriellen Schaden werden zudem in ErwG 85 der DSGVO zur Begründung der strengen Meldepflichten genannt:

„*Die Risiken für die Rechte und Freiheiten natürlicher Personen [...] können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn [...] die betroffenen Personen [...] daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren [...]*“

Daraus ergibt sich, dass bereits der Verlust der Kontrolle über personenbezogene Daten einen immateriellen Schaden im Sinne der Verordnung darstellt. Vor diesem Hintergrund mehren sich die Entscheidungen, in denen Gerichte einen entsprechenden Schadenersatzanspruch aufgrund eines Kontrollverlustes oder einer Einschränkung der Betroffenenrechte bejaht haben. So führte das ArbG Dresden in einem Urteil vom 26.08.2020 [Az.: 13 Ca 1046/20, ZD 2021, 54] aus:

„*Der Begriff des Schadens ist auf eine Art und Weise auszulegen, die den Zielen der DS-GVO in vollem Umfange entspricht. Insoweit ist durch das Inkrafttreten der DS-GVO eine Verschärfung im Vergleich zur bisherigen Rechtslage eingetreten. Ein immaterieller Schaden entsteht nicht nur in den, auf der Hand liegenden Fällen', wenn die datenschutzwidrige Verarbeitung zu einer Diskriminierung, einem Verlust der Vertraulichkeit, einer Rufschädigung oder anderen gesellschaftlichen Nachteilen führt, sondern auch, wenn die betroffene Person um ihre Rechte und Freiheiten gebracht oder daran gehindert ist, die sie betreffenden personenbezogen Daten zu kontrollieren.*“

Weiterhin stützten auch das LG Darmstadt [Urteil vom 26.05.2020, Az.: 13 O 244/19, ZD 2020, 642] sowie das LG Lüneburg [Urteil vom 14.07.2020, Az.: 9 O 145/19, BeckRS 2020, 36932] die von ihnen ausgeurteilten Schadenersatzansprüche auf einen Verlust der Kontrolle über die betroffenen personenbezogenen Daten, obwohl sich in beiden Fällen die dadurch gesetzte Gefahr der Rufschädigung nicht realisiert hatte. Das LG Lüneburg führt für das Vorliegen eines immateriellen Schadenersatzanspruchs insbesondere aus:

„*Dafür bedarf es entgegen der Ansicht der Beklagten nicht die in der bisherigen deutschen Rechtsprechung für Schmerzensgeld geforderte Voraussetzung einer schwerwiegenden*

Persönlichkeitsverletzung, welche sich nicht mit Art. 82 DS-GVO verträgt. Sie ist weder vorgesehen noch von dessen Ziel und Entstehungsgeschichte gedeckt *(Quaas, in: BeckOK DatenschutzR, Art. 82 DS-GVO, Rn. 32). Der Anspruch ist hiervon grundsätzlich unabhängig. Für diese Ansicht spricht auch der Erwägungsgrund 85 S. 1 der DS-GVO. Danach kann eine Verletzung des Schutzes personenbezogener Daten einen immateriellen Schaden für natürliche Personen nach sich ziehen, wie etwa den Verlust der Kontrolle über ihre personenbezogenen Daten. Für eine weite Auslegung des Schadensbegriffs spricht zudem der Erwägungsgrund 146 S. 6 der DS-GVO, wonach der Betroffene einen vollständigen und wirksamen Schadenersatz für den erlittenen Schaden erhalten soll. Die schwerwiegende Persönlichkeitsverletzung könnte vor diesem Hintergrund auch nicht als untere Grenze einer Schmerzensgeldhöhe wieder eingelesen werden. Vielmehr ist der immaterielle Schaden umfassend zu ersetzen. Eine schwerwiegende Persönlichkeitsverletzung würde jedoch regelmäßig zu einem hohen Schmerzensgeld führen (Quaas, in: BeckOK DatenschutzR, 31. Ed, 1.2.2020, DS-GVO Art. 82 Rn. 31, 32). Insbesondere bei der Zugänglichmachung von Daten einer betroffenen Person für Dritte ohne ihr Einverständnis wird ein Schadenersatzanspruch auch einen immateriellen Schaden abzudecken haben, der diese öffentliche ‚Bloßstellung' kompensiert (Ehmann/Selmayr/Nemitz, 2. Aufl. 2018, DSGVO Art. 82 Rn. 13).*"

Das LG München stellte fest, dass Betroffene schon bei Übertragung der bloßen IP-Adresse an Unternehmen des Google-Konzerns in den USA aufgrund von Google Fonts einen entschädigungspflichtigen Kontrollverlust erleiden [LG München I, Urt. v. 20.1.2022 – 3 O 17493/20, ZD 2022, 290, Rn. 12]:

„Die Bekl. räumt ein, dass sie vor der Modifizierung ihrer Webseite bei den Besuchen des Kl. auf ihrer Webseite dessen IP-Adresse an Google übermittelt hat. Die Übermittlung der IP-Adresse erfolgte damit nicht nur einmalig. Der damit verbundene Eingriff in das allgemeine Persönlichkeitsrecht ist im Hinblick auf den Kontrollverlust des Kl. über ein personenbezogenes Datum an Google, ein Unternehmen, das bekanntermaßen Daten über seine Nutzer sammelt und das damit vom Kl. empfundene individuelle Unwohlsein so erheblich, dass ein Schadensersatzanspruch gerechtfertigt ist. Berücksichtigt werden muss dabei auch, dass unstreitig die IP-Adresse an einen Server von Google in den USA übermittelt wurde, wobei dort kein angemessenes Datenschutzniveau gewährleistet ist (vgl. EuGH Urt. v. 16.7.2020 – EUGH Aktenzeichen C31118 C-311/18 [= ZD 2020, ZD Jahr 2020 Seite 511 mAnm Moos/Rothkegel = MMR 2020, MMR Jahr 2020 Seite 597 mAnm Hoeren] – Facebook Ireland u. Schrems) und die Haftung aus Art. EWG_DSGVO Artikel 82 Abs. EWG_DSGVO Artikel 82 Absatz 1 DS-GVO präventiv weiteren Verstößen vorbeugen soll und Anreiz für Sicherungsmaßnahmen schaffen

soll.“

Vor diesem Hintergrund ist vorliegend ein immaterieller Schadenersatzanspruch im mindestens vierstelligen Bereich angemessen. Dies ergibt sich aus einem Vergleich mit anderen bereits ausgeurteilten Schadenersatzansprüchen:

- LG Darmstadt, Urt. v. 26.05.2020 – Az.: 13 O 244/19, ZD 2020, 642
  1.000 Euro für Verstoß gegen Art. 6 Abs. 1 DSGVO wegen unbefugter Offenlegung von Bewerberdaten an einen Dritten und Verstoß gegen Mittteilungspflicht aus Art. 34 DSGVO,
- LG Lüneburg, Urt. v. 14.07.2020 – Az.: 9 O 145/19, BeckRS 2020, 36932
  1.000 Euro für Verstoß gegen Art. 6 Abs. 1 DSGVO sowie Art. 17 Abs. 1 lit. d) DSGVO durch unzulässige Meldung einer Person bei einer Wirtschaftsauskunftei bei geringer Schuldsumme und relativ kurzer Dauer (1 Monat),
- ArbG Düsseldorf, Urt. v. 05.03.2020 – 9 Ca 6557/18, BeckRS 2020, 11910
  5.000 Euro für unvollständige und verspätete Auskunft nach Art. 15 Abs. 1 DSGVO und Verstoß gegen das Transparenzgebot nach Art. 12 Abs. 3 DSGVO,
- ArbG Neumünster, Urt. v. 11.08.2020 – 1 Ca 247 c/20, BeckRS 2020, 29998
  1.500 Euro für Verstoß gegen Art. 15 Abs. 1 DSGVO wegen verspäteter Beantwortung eines Auskunftsanspruchs (500 Euro pro Monat),
- OGH (Österreich), Urt. v. 23.06.2021 – 6 Ob 56/21k, abrufbar unter: https://noyb.eu/sites/default/files/2021-07/Teilurteil_S47-72_sw_de.pdf
  500 Euro wegen verspäteter und intransparenter Auskunft, wodurch der Betroffene „massiv genervt“ war (keine Vorlage an den EuGH, obwohl im selben Verfahren andere Fragen vorgelegt wurden).

2. Anspruch aus § 839 Abs. 1 Satz 1 BGB i. V. m. Art. 34 Satz 1 GG

Der Klägerin steht auch ein Anspruch aus § 839 Abs. 1 Satz 1 BGB i. V. m. Art. 34 Satz 1 GG zu.

a) Handeln in Ausübung eines öffentlichen Amtes

Die Angestellten der Beklagten handelten bei der Ausführung der Lehr- und Prüfungstätigkeit in Ausübung eines öffentlichen Amtes [vgl. Papier/Shirvani, Münchener Kommentar BGB, 8. Aufl. 2020 § 839 Rn. 220].

b) Verletzung einer drittbezogenen Amtspflicht

[1] Eine Amtspflicht kann sich auch aus Unionsrecht ergeben [Papier/Shirvani, Münchener Kommentar BGB, 8. Aufl. 2020 § 839 Rn. 263]. Vorliegend verstießen die Angestellten der Beklagten gegen die oben genannten Amtspflichten aus der DSGVO und dem TTDSG [siehe dazu Pkt. B. II. 1.]. Diese sind drittbezogen, da sie sich stets auf die personenbezogenen Daten bzw. die IT-Sicherheit der Betroffenen, also Individualinteressen beziehen.

[2] Vorliegend verletzen die Datenverarbeitungen die Klägerin in ihrem Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art 1 Abs. 1 GG. Dieses Recht schützt die Klägerin gegen die unbegrenzte Erhebung und Verarbeitung ihrer personenbezogenen Daten, um daraus resultierende Einschränkungen ihrer Handlungsfreiheit zu verhindern [BVerfG, Urteil vom 13.04.1983 – 1 BvR 209/83 – *Volkszählung* = NJW 1983, 1307 ff.].

Der Eingriff in das Recht auf informationelle Selbstbestimmung ist aus den oben genannten Gründen weder geeignet noch erforderlich.

[3] Die Installation und Ausführung des Programms *Lockdownbrowser* verletzt die Klägerin in ihrem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Laut dem BVerfG ist ein Eingriff anzunehmen,

„[…] wenn die Integrität des geschützten informationstechnischen Systems angetastet wird, indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können; dann ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen.“ [vgl. BVerfG, Urt. v. 27.2.2008 - 1 BvR 370/07, 1 BvR 595/07, Rn 204].

Das Grundrecht hat auch eine Schutzdimension. Den Staat trifft eine Pflicht, dazu beizutragen, dass die Integrität und Vertraulichkeit informationstechnischer Systeme gegen Angriffe durch Dritte geschützt werden [BVerfG, Beschluss des Ersten Senats vom 08.062021 - 1 BvR 2771/18 -, Rn. 33].

Mit diesen Anforderungen ist es unvereinbar, dass die Klägerin faktisch gezwungen war, den Lockdownbrowser auf ihrem privaten Endgerät zu installieren.

Der Lockdownbrowser infiltriert das Endgerät der Klägerin in einer Weise, die der Klägerin die Kontrolle über die Funktionsweise ihres Geräts aus der Hand nimmt und eine Manipulation des Systems von außen erlaubt.

c) Verschulden

Da den Entscheidungsträgern auf Seiten der Beklagten bei der Entschließung zum Einsatz von WISEflow bewusst war, dass dadurch eine biometrische Gesichtserkennung, ein Endgerätzugriff, eine automatisierte Entscheidungsfindung sowie Datentransfer in Drittländer veranlasst wird, handelten sie vorsätzlich.

d) Zurechenbarer Schaden

Die Klägerin erlitt aufgrund des Verlusts der Kontrolle über ihre biometrischen Daten, aufgrund des Stresses und der Ängste in der Prüfungssituation, aufgrund des Verlusts der Kontrolle über die an Dritte wie die *Google Ltd.* sowie die *Google LLC* weitergegebenen Daten sowie aufgrund des Verlusts des Vertrauens in die Vertraulichkeit und Integrität ihres Endgeräts einen erheblichen Schaden. Insbesondere die rechtswidrige Verarbeitung biometrischer Daten der Klägerin und die Übermittlung derselben an Unternehmen der Amazon-Gruppe stellt einen schweren Eingriff in ihr Persönlichkeitsrecht dar. [vgl. zur erheblichen Persönlichkeitsrechtsverletzung bei Übermittlung der bloßen IP-Adresse an Unternehmen des Google-Konzerns: LG München I, Urt. v. 20.01.2022 – 3 O 17493/20, ZD 2022, 290, Rn. 12].

Sollte das Gericht den bisherigen Sachvortrag oder die bisherigen Beweisangebote der Klägerin nicht für ausreichend erachten, oder die hier vertretene Rechtsauffassung nicht teilen, so wird ausdrücklich um einen entsprechenden - ggf. telefonischen - Hinweis gemäß § 139 ZPO gebeten.

Die Übermittlung des Schriftsatzes erfolgt im elektronischen Rechtsverkehr und ausdrücklich im Namen der Kanzlei Spirit Legal Fuhrmann Hense Partnerschaft von Rechtsanwälten. Aufgrund der elektronischen Übersendung per EGVP/beA/De-Mail sind Abschriften nicht beigefügt (§ 133 Abs. 1 S. 2 ZPO). Für die rechtsgültige Unterschrift siehe Empfangs- und Signaturprotokoll Ihrer empfangenden Fernmeldeanlage.

Elisabeth Niekrenz

Rechtsanwältin

Peter Hense

Rechtsanwalt

Anlagen:

Anlage K 1	Auskunft der Beklagten vom 03.12.2021
Anlage K 2	Anlage zur Auskunft der Beklagten vom 24.03.2022: Datenübersicht zum Auskunftsverlangen 21/806/ENK/CSC, S. 84
Anlage K 3	Teilausdruck der Website der *UNIwise* ApS. vom 12.07.2022
Anlage K 4	Schreiben der Beklagten vom 24.03.2022
Anlage K 5	Anlage zur Auskunft der Beklagten vom 03.12.2021: Bild-Protokoll Fernklausur EKK 22.07.2021
Anlage K 6	Anleitung der Beklagten zur Durchführung von rechtssicheren und datenschutzkonformen elektronischen Prüfungen vom 14.09.2021
Anlage K 7	Anlage zur Auskunft der Beklagten vom 03.12.2021: Accountansicht_...
Anlagenkonvolut K 8	Bildprotokolle der einzelnen Prüfungen
Anlage K 9	Teilausdruck der Website der Google Ireland Ltd, abrufbar unter: https://marketingplatform.google.com/intl/de/about/tag-manager/features/, abgerufen am 19.10.2022
Anlage K 10	Teilausdruck der Website der Google Ireland Ltd, abrufbar unter: https://developers.google.com/tag-platform/tag-manager/server-side, abgerufen am 19.10.2022
Anlage K 11	von der Beklagten übermittelte Aufstellung: WISEflow Subprocessors
Anlage K 12	Standard Contractual Clauses, Data Processing Agreement WISEflow/Universität Erfurt vom 15.12.2021
Anlage K 13	Datenschutzerklärung der Beklagten zur Nutzung von Wiseflow, Stand: März 2022
Anlage K 14	Aufforderungsschreiben der Klägerin vom 24.05.2022