Beglaubigte Abschrift

Hanseatisches Oberlandesgericht

Az.: 5 UKl 1/25

Verkündet am 13.05.2026

JFAng
Urkundsbeamter der Geschäftsstelle

Urteil

IM NAMEN DES VOLKES

In der Sache

Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V., vertreten durch die Vorständin Rudi-Dutschke-Straße 17, 10969 Berlin

- Kläger -

Prozessbevollmächtigte:

gegen

aestimium GmbH, vertreten durch den Geschäftsführer Rödingsmarkt 39, 20459 Hamburg

- Beklagte -

Prozessbevollmächtigte:

erkennt das Hanseatische Oberlandesgericht - 5. Zivilsenat - durch den Vorsitzenden Richter am Oberlandesgericht den Richter am Oberlandesgericht und die Richterin am Oberlandesgericht auf Grund der mündlichen Verhandlung vom 15.04.2026 für Recht:

1. Die Klage wird abgewiesen.
2. Die Kosten des Rechtsstreits hat der Kläger zu tragen.
3. Das Urteil ist hinsichtlich der Kosten vorläufig vollstreckbar.
4. Die Revision wird nicht zugelassen.

Tatbestand

Die Parteien streiten über die Wirksamkeit Allgemeiner Geschäftsbedingungen bezüglich der

Verarbeitung biometrischer Daten.

Der Kläger ist in die Liste qualifizierter Einrichtungen gemäß § 4 Abs. 1 UKlaG des Bundesamts für Justiz eingetragen.

Das Geschäftsmodell der Beklagten ist die Bereitstellung von Ergebnissen aus Umfragen und Tests für ihre Geschäftspartner. Solche Geschäftspartner können z. B. Vertreiber von mobilen Applikationen oder Anbieter von Handyspielen oder von Internetseiten sein. Dafür unterhält die Beklagte unter https://www.empfohlen.de/ eine Plattform, deren Nutzer (Mitglieder) sich registrieren und anschließend an durch Geschäftspartner beauftragten Umfragen und Tests teilnehmen können. Dabei kann es sich z.B. um Umfragen zu Themen wie Sport und Fitness oder um Tests von mobilen Applikationen, Internetseiten oder Handyspielen handeln. Wenn Mitglieder Umfragen/Tests durchführen, wird dem jeweiligen Mitgliedsaccount ein dafür jeweils festgelegtes Guthaben (in Euro) gutgeschrieben; Mitglieder können sich dieses Guthaben jederzeit auszahlen lassen.

Durch die automatisierte Teilnahme mittels sogenannter Bots und durch die mehrfache Registrierung desselben Mitglieds bei den Umfragen und Tests können unbrauchbare oder verzerrte Ergebnisse entstehen. Daher führt die Beklagte, bevor sie Guthaben an Mitglieder auszahlt, einen sogenannten Liveness Check durch. Dabei wird ein Gesichtsbild des Mitglieds aufgenommen; dies erfolgt regelmäßig über die Kamera des Mobilgeräts des Mitglieds. Das Gesichtsbild wird dann verwendet, um zu prüfen, ob der Auszahlungsprozess durch einen Menschen (also nicht automatisiert) veranlasst wurde (erste Komponente des Liveness Checks) und ob dasselbe Mitglied in der Vergangenheit bereits eine Auszahlung für einen anderen Mitgliedsaccount veranlasst hat (zweite Komponente des Liveness Checks).

Im Rahmen der ersten Komponente des Liveness Checks wird das Gesichtsbild anhand von Merkmalen und Ankerpunkten eines menschlichen Gesichts (z. B. Position der Augen) analysiert, um festzustellen, ob eine natürliche Person den Auszahlungsvorgang angestoßen hat. Für die zweite Komponente des Liveness Checks wird das Gesichtsbild in einen sogenannten 3D FaceVector konvertiert. Das ist eine aus Merkmalen und Ankerpunkten des Gesichtsbilds generierte Nummernabfolge. Dieser 3D FaceVector (und nicht das Gesichtsbild) wird dann mit 3D FaceVectoren abgeglichen, welche im Rahmen des Liveness Checks anderer Mitgliedsaccounts erstellt wurden. Wenn der 3D FaceVector im Rahmen eines Liveness Checks identisch mit einem abgeglichenen 3D FaceVector ist, ergibt sich daraus, dass die entsprechende Person den Liveness Check bereits für einen anderen Mitgliedsaccount

durchgeführt hat. Das Gesichtsbild selbst wird hingegen nicht aufbewahrt. Gespeichert wird lediglich das Ergebnis des Liveness Checks, der Zeitpunkt, zu welchem dieser durchgeführt wurde und der 3D FaceVector. Der 3D FaceVector wird dabei keinem Mitgliedsaccount zugeordnet und kann daher grundsätzlich keiner Person mehr zugeordnet werden.

Teil 2 § 2 Abs. 3 der Empfohlen-AGB der Beklagten stellt klar, dass eine höchstpersönliche Teilnahme an Umfragen/Tests erforderlich ist und schließt eine Teilnahme mittels Bots oder anderer Spam-Software sowie unter fremder Identität aus:

„(...) *Die Teilnahme an Bewertungen und Umfragen darf nur durch das Mitglied höchstpersönlich erfolgen. Die Teilnahme mittels Bots oder anderer Spam-Software sowie unter fremder Identität ist ausdrücklich untersagt.*"

Aus Teil 1 § 1 Abs. 2 der Empfohlen-AGB ergibt sich außerdem, dass jedes Mitglied nur einen Mitgliedsaccount unterhalten darf:

„(...) *Jedes Mitglied darf zeitgleich nur einen Mitgliedsaccount unterhalten*."

Außerdem werden Mitglieder ausdrücklich mittels eines Banners über den Liveness Check informiert, wenn sie sich in ihren Mitgliedsaccount einloggen. Das Banner weist darauf hin, dass im Rahmen des Auszahlungsvorgangs ein Liveness Check vorgenommen werden kann. Es wird am oberen Rand des Browsers / der App angezeigt, bis das Mitglied das Banner per Klick auf einen Button („Verstanden") bestätigt (Anlage B 4).

Die Beklagte verwendet unter der URL https://www.empfohlen.de/agb/ in ihren Allgemeinen Geschäftsbedingungen (Geltung ab dem 11.07.2023) die nachfolgende Klausel, die vom Kläger beanstandet wird. Dort heißt es im Teil 2 unter § 3 Abs. 4:

(Teil 2: Besondere Bestimmung für die Nutzung des Moduls „Geld verdienen"

§ 3 Vergütung)

[...]

(4) Zur Betrugsprävention (insbesondere zum Ausschluss von Bots und anderer Spam-Software) kann der Anbieter vor einer Auszahlung vom Mitglied einen Identitäts-/Existenznachweis mittels eines vom Anbieter dazu angebotenen Verfahrens („Nachweis-Verfahren") fordern. Das Nachweis-Verfahren kann die Erfassung und Verarbeitung biometrischer Daten beinhalten. Solange das Mitglied das Nachweis-Verfahren

nicht erfolgreich abgeschlossen hat, kann der Anbieter die Auszahlung verweigern (weitere Rechte des Anbieters nach diesen AGB bleiben unberührt).

In Ziffer III.1.d) des von der Beklagten unter der URL https://www.empfohlen.de/datenschutz/ einsehbaren Datenschutzhinweises erläutert die Beklagte das von ihr angebotene Nachweisverfahren (Anlage K 1). Weitere Informationen werden unter der URL https://support.empfohlen.de/hc/de/categories/12975029509660-Auszahlung in den dort vorgehaltenen FAQs (Anlage K 2) gegeben.

Unter der URL https://support.empfohlen.de/hc/de/articles/9429328140572-Wie-funktioniert-die-Verifizierung-3D-Liveness-Check stellt die Beklagte folgende Informationen zur Verfügung (Anlagenkonvolut K 3):

„Wenn du das nächste Mal eine Auszahlung in deinem empfohlen.de-Konto beantragst, wirst du möglicherweise zu einem 3D Liveness Check aufgefordert, um deine Lebensechtheit festzustellen. Klicke einfach auf „Verifiziere dich", um fortzufahren.

Bevor du den 3D Liveness Check starten kannst, erfragen wir deine aktive Einwilligung. Wurde die Einwilligung erteilt, dann startet der 3D Liveness Check direkt auf empfohlen.de."

Der Kläger mahnte die Beklagte mit Schreiben vom 20.08.2024 wegen Verwendung der oben genannten Klausel in Teil 2 unter § 3 Abs. 4 der AGB sowie wegen weiterer nicht streitgegenständlicher Verstöße ab (Anlage K 4). Die Beklagte gab am 29.10.2024 lediglich hinsichtlich der anderen Verstöße eines strafbewehrte Unterlassungserklärung ab (Anlage K 5).

Der Kläger ist der Meinung, dass die Verwendung dieser Klausel einen Verstoß gegen § 1 UKlaG i.V.m. § 307 Abs. 1 S. 1, Abs. 2 Nr. 1 BGB i.V.m. Art. 9 Abs. 1, Abs. 2 lit. a DSGVO darstelle. Die angegriffene Bestimmung weiche von wesentlichen Grundgedanken des Art. 9 Abs. 2 lit. a DSGVO ab. Eine Einwilligung nach Art. 9 Abs. 2 lit. a DSGVO in die Verarbeitung biometrischer Daten baue auf den allgemeinen Anforderungen an die Einwilligung aus Art. 4 Nr. 11, Art. 7 und Art. 8 DSGVO auf. Damit sei die Freiwilligkeit der Einwilligung eine der Voraussetzungen für die rechtmäßige Verarbeitung der biometrischen Daten der Mitglieder.

Nach dem Erwägungsgrund 42 Satz 5 zur DSGVO solle nur dann davon ausgegangen werden, dass die betroffene Person ihre Einwilligung freiwillig gegeben habe, wenn sie eine echte oder freie Wahl habe und somit in der Lage sei, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden. Die Beklagte knüpfe in der angegriffenen Klausel aber eine negative

Folge an die fehlende Erteilung einer Einwilligung für die Mitglieder. Danach könne die Beklagte die Auszahlung des Kontoguthabens verweigern, solange das Mitglied das Nachweisverfahren nicht erfolgreich abgeschlossen habe. Darüber hinaus stelle die Beklagte - was unstreitig ist - keine Alternative zu dem von der Beklagten gewählten Nachweisverfahren zur Verfügung. Mitglieder hätten also keine Wahlmöglichkeit.

Zudem sei die Überlegung der Beklagten, dass eine vertragswidrige Teilnahme am besten verhindert werden könne, wenn das vertragswidrige Verhalten nicht profitabel sei, nicht nachvollziehbar. Denn die Beklagte könne schon viel früher Maßnahmen zum Schutz vor vertragswidriger Teilnahme ergreifen. So könne die Verfälschung der Resultate der Umfragen durch Verwendung von Bots und durch die mehrfache Teilnahme verhindert werden, wenn die Identität bereits bei der Registrierung geprüft werde. Der Kläger trägt ferner vor, dass der Liveness Check nicht das einzig verfügbare Mittel sei, um die genannten Risiken zu reduzieren. Es gebe auch andere Methoden, die weniger in die Persönlichkeitsrechte eingriffen (z.B. Captcha-Lösungen, Versendung von Zugangslinks, die nur einmalig funktionierten, sogenannte Honeypot-Felder, die nur von Bots ausgefüllt würden). Auch werde mit Nichtwissen bestritten, dass problemlos und kostenlos eine Vielzahl verschiedener E-Mail-Adressen eingerichtet werden könne. Es sei außerdem in rechtlicher Hinsicht unerheblich, ob es ein gleich effektives Mittel gebe, denn maßgeblich sei, ob die streitgegenständliche Verarbeitung rechtmäßig sei.

Die Einwilligung der Mitglieder werde demnach nicht freiwillig erteilt. Die Erhebung der biometrischen Daten der Mitglieder erfolge deshalb ohne Rechtsgrundlage. Damit liege ein Verstoß gegen § 1 UKlaG i.V.m. § 307 Abs. 1 S. 1, Abs. 2 Nr. 1 BGB i.V.m. Art. 9 Abs. 1, Abs. 2 lit. a DSGVO vor.

Der Kläger ist ferner der Ansicht, dass die angegriffene Klausel nach § 307 Abs. 1 S. 1 BGB unwirksam sei. Die Beklagte versuche durch eine einseitige Vertragsgestaltung missbräuchlich eigene Interessen auf Kosten ihres Vertragspartners durchzusetzen, ohne von vornherein auch dessen Belange hinreichend zu berücksichtigen und dem Vertragspartner einen angemessenen Ausgleich zuzugestehen. Das Interesse des Identitätsnachweises vor einer Auszahlung stehe in keinem Verhältnis zur erforderlichen Preisgabe der biometrischen Daten der Mitglieder.

Die Verarbeitung von biometrischen Daten könne auch nicht auf Art. 6 Abs. 1 lit. f DSGVO gestützt werden, weil dies keine taugliche Rechtsgrundlage sei.

Der Kläger hat zuletzt beantragt,

die Beklagte zu verurteilen, es bei Vermeidung eines für jeden Fall der Zuwiderhandlung festzusetzenden Ordnungsgeldes bis zu 250.000,00 €, ersatzweise Ordnungshaft bis zu sechs Monaten oder Ordnungshaft bis zu sechs Monaten, zu vollstrecken an der Geschäftsführung, künftig zu unterlassen, im Rahmen geschäftlicher Handlungen gegenüber Verbraucher:innen in Verträgen über die Online-Teilnahme an Umfragen und Tests nachfolgende oder inhaltsgleiche Klauseln zu verwenden:

(Teil 2: Besondere Bestimmung für die Nutzung des Moduls „Geld verdienen"

§ 3 Vergütung)

[...]

(4) Zur Betrugsprävention (insbesondere zum Ausschluss von Bots und anderer Spam-Software) kann der Anbieter vor einer Auszahlung vom Mitglied einen Identitäts-/Existenznachweis mittels eines vom Anbieter dazu angebotenen Verfahrens („Nachweis-Verfahren") fordern. Das Nachweisverfahren kann die Erfassung und Verarbeitung biometrischer Daten beinhalten. Solange das Mitglied das Nachweisverfahren nicht erfolgreich abgeschlossen hat, kann der Anbieter die Auszahlung verweigern (weitere Rechte des Anbieters nach diesen AGB bleiben unberührt).

Die Beklagte beantragt,

die Klage abzuweisen.

Die Beklagte ist der Ansicht, dass die streitgegenständliche Klausel nicht den wesentlichen Grundgedanken der DSGVO widerspreche und auch sonst zu keiner unangemessenen Benachteiligung führe.

Die Beklagte ist der Meinung, dass der Liveness Check nicht gegen die DSGVO verstoße. Nach Kenntnis der Beklagten sei kein anderes gleich effektives Mittel verfügbar, mit dem sich die Beklagte vor Missbrauch durch automatisierte Durchführung oder Mehrfachteilnahme an Umfragen/Tests schützen könne. Insbesondere böten etwa Captchas keinen angemessenen Schutz (mehr) vor Bots. Die Beklagte verweist insoweit auf das Online-Fachmagazin golem.de, das bereits 2023 festgestellt habe, dass Bots Captchas inzwischen schneller lösten als Menschen (Anlage B 1). Durch die Nutzung künstlicher Intelligenz ließen sich Bots dergestalt zur Durchführung von Umfragen programmieren, dass sie auch andere typische Schutzmaßnahmen

gegen Botmissbrauch umgehen könnten. Das gelte insbesondere für sogenannte Honeypot-Fragen; dies sind Fragen, welche in weißem Text auf weißem Hintergrund dargestellt werden und von Menschen übersprungen werden, da sie für diese nicht sichtbar sind. Die Beklagte verweist insoweit auf eine Studie (Anlage B 2). Auch Maßnahmen wie die Begrenzung auf einen Mitgliedsaccount pro E-Mail-Adresse böten keinen hinreichend wirksamen Schutz. Bei verschiedenen E-Mail-Anbietern (z. B. Gmail, web.de, gmx.de, yahoo) könnten problemlos und kostenlos eine Vielzahl verschiedener E-Mail-Adressen eingerichtet werden oder zusätzliche Alias-E-Mail-Adressen für eine E-Mail-Adresse hinterlegt werden, um eine solche Begrenzung leicht zu umgehen.

Auch Zugangslinks, die nur einmal verwendet werden könnten, böten nicht hinreichend Schutz vor automatisierter Durchführung oder Mehrfachteilnahmen an Umfragen/Tests auf der Plattform.

Die Beklagte stützt sich bei der ersten Komponente des Liveness Checks auf die Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO) und bei der zweiten Komponente des Liveness Checks auf die ausdrückliche Einwilligung ihrer Mitglieder nach Art. 9 Abs. 2 lit. a DSGVO. Die Beklagte könne für diese Verarbeitung ausdrückliche Einwilligungen wirksam einholen. Insbesondere seien diese Einwilligungen freiwillig erteilt im Sinne von Art. 4 Nr. 11 DSGVO. Insoweit sei zu berücksichtigen, dass Art. 7 Abs. 4 DSGVO nach allgemein vertretener Ansicht kein absolutes, sondern lediglich ein relatives Kopplungsverbot enthalte. Danach finde Art. 7 Abs. 4 DSGVO keine Anwendung, wenn die in Frage stehende Einwilligung eine Datenverarbeitung legitimiere, die für die Erfüllung des Vertrags, in dessen Zusammenhang sie eingeholt werde, erforderlich sei. Dies sei im Streitfall zu bejahen. Denn die Durchführung des Liveness Checks sei existenziell für die Aufrechterhaltung des Geschäftsmodells der Beklagten. Nur so könne die Beklagte sicherstellen, dass die unter den Empfohlen-AGB geschuldete höchstpersönliche Leistung vertragskonform ohne die Nutzung von Bots und anderer Spam-Software erbracht werde und kein Missbrauch der Plattform durch automatisierte Teilnahme an Umfragen/Tests sowie Mehrfachteilnahmen erfolge. Ein vergleichbares Beispiel sei das Erfordernis von Versicherungen, Einwilligungen in die Verarbeitung von Gesundheitsdaten einzuholen.

Selbst wenn man dennoch annehmen wolle, dass die Erforderlichkeit der Datenverarbeitung zur Vertragsdurchführung zu verneinen sei, so greife das relative Kopplungsverbot aus Art. 7 Abs. 4 DSGVO im vorliegenden Fall gleichwohl nicht ein. Denn anhand des Gesamtkontexts werde deutlich, dass die Einwilligung der Nutzer freiwillig erteilt werde. Die Beklagte meint, die freie Wahlmöglichkeit der Mitglieder hinsichtlich des Umgangs mit ihren personenbezogenen Daten bleibe trotz des Erfordernisses eines Liveness Checks bestehen. Die Verarbeitung der

biometrischen Daten im Rahmen des Liveness Checks sei von geringer Intensität. Darüber hinaus bestehe zwischen der Beklagten als Anbieterin der Plattform und den Mitgliedern keineswegs ein klares Ungleichgewicht, insbesondere habe die Beklagte - was unstreitig ist - keine Monopolstellung am Markt inne. Die Beispiele, in denen eine derartige Monopolstellung Auswirkungen auf die Freiwilligkeit habe, seien vorliegend offensichtlich nicht einschlägig.

Überdies finde im Rahmen der Erteilung der Einwilligung ein angemessener Interessenausgleich im Sinne von § 307 Abs. 1 Satz 1 BGB statt. Zunächst sei festzuhalten, dass kein gleichwertiges und milderes Mittel vorhanden sei als der Liveness Check, um sicherzustellen, dass die Plattform nicht durch Automatisierung (z. B. mittels Bots) und Mehrfachteilnahmen an Umfragen/Tests vertragswidrig zur Erwirtschaftung von Geld missbraucht werde. Die Kopplung sei auch im engeren Sinne verhältnismäßig. Schließlich sei die Erteilung der Einwilligung nicht nur für die Beklagte selbst von Vorteil. Auch die Mitglieder profitierten davon, weil die Beklagte andernfalls ihren Mitgliedern voraussichtlich nicht die Möglichkeit bieten könne, mittels der Teilnahme an Umfragen/Tests Geld zu verdienen.

Soweit der Kläger meine, dass die Beklagte die Identität der Mitglieder bereits bei der Registrierung überprüfen könne, so träfe dies auch solche Mitglieder, die sich zwar für die Plattform registriert hätten, aber nie Guthaben erwirtschaftet hätten. Indem die Beklagte den Liveness Check erst durchführe, wenn ein Mitglied den Auszahlungsprozess veranlasse, werde sichergestellt, dass personenbezogene Daten nur im erforderlichen Rahmen verarbeitet würden, nämlich von Mitgliedern, die sich für eine Auszahlung qualifizierten und eine solche begehrten.

Wegen des weiteren Vortrags der Parteien wird auf die eingereichten Schriftsätze nebst Anlagen sowie auf das Sitzungsprotokoll vom 15.04.2026 Bezug genommen.

Entscheidungsgründe

Die Klage ist zulässig, aber unbegründet.

I. Die Klage ist zulässig.

1. Die Klage ist bei dem gemäß § 6 Abs. 1 S. 1 UKlaG zuständigen Gericht erhoben worden. Gemäß § 6 Abs. 1 S. 3 UKlaG entscheidet das Oberlandesgericht nach den für das erstinstanzliche Verfahren geltenden Vorschriften.

2. Der Klageantrag ist hinreichend bestimmt im Sinne des § 253 Abs. 2 Nr. 2 ZPO. Streitgegenstand ist nicht der „Liveness Check“ selbst, sondern nur die im Klageantrag

wiedergegebene Regelung in Teil 2 § 3 Abs. 4 der AGB der Beklagten bezüglich des Nachweisverfahrens.

II. Die Klage ist unbegründet. Dem Kläger steht gegen die Beklagte der geltend gemachte Unterlassungsanspruch nach § 1 UKlaG wegen Verwendung einer nach § 307 Abs. 1 oder Abs. 2 BGB unwirksamen Bestimmung in Allgemeinen Geschäftsbedingungen nicht zu.

1. Der Kläger ist anspruchsberechtigt nach § 3 Abs. 1 S. 1 Nr. 1 UKlaG. Er ist als qualifizierter Verbraucherverband in der entsprechenden vom Bundesamt für Justiz geführten Liste eingetragen. Qualifizierten Einrichtungen steht auch gemäß § 3 Abs. 1 Satz 1 Nr. 1 UKlaG die Befugnis zu, gegen DSGVO-Verstöße im Rahmen der Verwendung von unwirksamen Allgemeinen Geschäftsbedingungen gemäß § 1 UKlaG im Wege einer Klage vor den Zivilgerichten vorzugehen (vgl. BGH GRUR 2025, 653, 655 Rn. 27ff. - App-Zentrum III).

2. Nach § 1 UKlaG kann, wer in Allgemeinen Geschäftsbedingungen Bestimmungen, die nach den §§ 307 bis 309 BGB unwirksam sind, verwendet oder für den rechtsgeschäftlichen Verkehr empfiehlt, auf Unterlassung und im Fall des Empfehlens auch auf Widerruf in Anspruch genommen werden. Eine solche Unwirksamkeit ist bei der in Streit stehenden Klausel zu verneinen.

a. Bei der streitgegenständlichen Regelung in Teil 2 § 3 Abs. 4 handelt es sich um eine für eine Vielzahl von Verträgen vorformulierte Vertragsbedingung, die die Beklagte ihren Vertragspartnern bei Abschluss eines Vertrages stellt, mithin um eine Allgemeine Geschäftsbedingung gemäß § 305 Abs. 1 S. 1 BGB.

b. Zu den gesetzlichen Regelungen im Sinne von § 307 Abs. 2 Nr. 1 BGB zählen auch die Vorschriften der DSGVO, insbesondere die Regelungen über die Rechtmäßigkeit der Datenverarbeitung in den Fällen des Art. 6 Abs. 1 DSGVO (OLG Köln, Urteil vom 03.11.2023 – I-6 U 58/23 –, Rn. 65, juris). Gleiches gilt auch für den vorliegend geltend gemachten Verstoß gegen Art. 9 DSGVO.

c. Die angegriffene Klausel verstößt nicht gegen die Regelungen der DSGVO, insbesondere nicht gegen Art. 9 Abs. 1, Abs. 2 lit. a DSGVO.

aa. Nach Art. 9 Abs. 1 DSGVO ist u.a. die Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person untersagt. Nach Art. 9 Abs. 2 lit. a DSGVO gilt das Verbot nach Art. 9 Abs. 1 DSGVO nicht, wenn die betroffene Person in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt

hat, es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden.

bb. In der angegriffenen Klausel ist die Verarbeitung biometrischer Daten im Sinne von Art. 9 Abs. 1 DSGVO geregelt. Denn dort ist bestimmt, dass das Nachweisverfahren die Erfassung und Verarbeitung biometrischer Daten beinhalten kann.

cc. Nach Art. 4 Nr. 11 DSGVO ist „Einwilligung" der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Nach Art. 7 Abs. 4 DSGVO muss bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.

dd. Ein Verstoß gegen Art. 9 Abs. 1, Abs. 2 lit. a DSGVO ist im Streitfall entgegen der Auffassung des Klägers zu verneinen, weil eine im Rahmen des Nachweisverfahrens (Liveness Check) vor der Auszahlung der erwirtschafteten Beträge eingeholte Einwilligung der Mitglieder der Beklagten in die Verarbeitung biometrischer Daten freiwillig und damit wirksam ist.

ee. Art. 7 Abs. 4 DSGVO regelt unter dem Gesichtspunkt der Freiwilligkeit einen Sonderfall, das Koppelungsverbot. Der Gesetzgeber will nicht absolut die Koppelung verbieten, sondern nur für den Regelfall. Es muss „in größtmöglichem Umfang" berücksichtigt werden, ob die Erfüllung des Vertrags bei seinem Abschluss von einer Einwilligung zu einer Datenverarbeitung abhängig gemacht worden ist, die für die Erfüllung des Vertrags nicht erforderlich war. Hierbei ist auf die konkreten Umstände des Einzelfalls abzustellen (Hans-Jürgen Schaffland; Gabriele Holthaus in: Schaffland/Wiltfang, Datenschutz-Grundverordnung (DS-GVO)/Bundesdatenschutzgesetz (BDSG), Februar 2026, Art. 7 EUV 2016/679, Rn. 67).

ff. Die Beklagte macht in der angegriffenen Klausel die Erfüllung ihrer Verträge mit den Mitgliedern von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig im Sinne von Art. 7 Abs. 4 DSGVO. Erfüllung des Vertrages im Sinne von Art. 7 Abs. 4 DSGVO meint in erster Linie die Erfüllung vertraglich begründeter Haupt- und Nebenpflichten, aber auch und gerade den Vertragsabschluss (Hans-Jürgen Schaffland; Gabriele Holthaus in: Schaffland/Wiltfang, Datenschutz-Grundverordnung (DS-GVO)/Bundesdatenschutzgesetz (BDSG), Februar 2026,

Art. 7 EUV 2016/679, Rn. 67; vgl. ferner zu Art. 6 DSGVO: Gola/Heckmann/Schulz, 3. Aufl. 2022, DS-GVO Art. 6 Rn. 30). Im Streitfall ist die Auszahlung der vertraglich geschuldeten Vergütung, mithin die Erfüllung der Zahlungspflicht der Beklagten gegenüber ihren Mitgliedern, von der Einwilligung der Mitglieder in die Verarbeitung biometrischer Daten abhängig.

gg. Die Verarbeitung biometrischer Daten ist im vorliegenden Fall zur Erfüllung des Vertrages zwischen den Mitgliedern und der Beklagten erforderlich, so dass eine im Rahmen des Nachweisverfahrens zu erteilende Einwilligung unter Berücksichtigung der Gesamtumstände als freiwillig anzusehen ist.

aaa. Im Grundsatz trägt die Beklagte als Verantwortliche die Darlegungs- und Beweislast für die Erforderlichkeit der von ihr vorgenommenen Datenverarbeitung (vgl. BGH, Urteil vom 18.12.2025 – I ZR 97/25 –, Rn. 45, juris).

bbb. Dem ist die Beklagte nachgekommen. Das Nachweisverfahren hat den Zweck, sicherzustellen, dass die Mitglieder ihre Verpflichtung zur höchstpersönlichen Teilnahme gemäß Teil 2 § 2 Abs. 3 der AGB erfüllen und nicht gegen das Verbot der Mehrfachregistrierung in Teil 1 § 1 Abs. 2 der AGB verstoßen. Anhaltspunkte dafür, dass diese Klauseln unwirksam sein könnten, sind weder vorgetragen noch sonst ersichtlich. Das Nachweisverfahren dient also der Sicherstellung der ordnungsgemäßen Erfüllung der Vertragspflichten der Mitglieder und der Verhinderung von Betrug. Daran hat die Beklagte ein schützenswertes Interesse, da sie ihren Vertragspartnern verwertbare Ergebnisse aus Tests und Umfragen schuldet und das Risiko einer Verfälschung der Ergebnisse durch Bots und Mehrfachteilnahme besteht. Das Nachweisverfahren ist auch geeignet, Betrugsfälle zu verhindern, insbesondere in Verbindung mit den von der Beklagten im Vorfeld (u.a. mittels Banner) erteilten Hinweisen, dass vor der Auszahlung ein Liveness Check durchgeführt werden kann.

Soweit der Kläger einwendet, dass die Beklagte die Identität der Mitglieder bereits bei der Registrierung überprüfen könne, steht dies nicht der Erforderlichkeit der Verarbeitung biometrischer Daten im Rahmen des Nachweisverfahrens entgegen. Denn unstreitig gibt es auch Mitglieder, die sich auf der Plattform der Beklagten registrieren, aber kein Guthaben erwirtschaften. Indem die Beklagte erst im Rahmen der Auszahlung biometrische Daten erhebt, wird sie dem Grundsatz der Datensparsamkeit gerecht.

Auch gibt es im Streitfall keine wirksamen milderen Mittel zur Verhinderung der Mehrfachteilnahme und des Einsatzes von Bots. Soweit es um den Ausschluss von Bots geht, hat der Kläger die durch die Anlagen B 1 und B 2 substantiierte Behauptung der Beklagten, dass

Maßnahmen wie Captchas und Honeypot-Felder gegenüber Bots nicht (mehr) wirksam seien, nicht ausreichend bestritten. Hinsichtlich der mehrfachen Registrierung von Mitgliedern hat der Kläger mit Nichtwissen bestritten, dass problemlos und kostenlos eine Vielzahl von verschiedenen E-Mail-Adressen eingerichtet werden könne und hat vorgetragen, dass jedenfalls bei GMX eine gültige Mobilfunknummer angegeben werden müsse und bei Gmail und Yahoo eine Telefonnummer zur Verifizierung mit einem Code erforderlich sei. Dies schließt jedoch nicht aus, dass bei einem Anbieter wie GMX zur Verifizierung einer weiteren E-Mail-Adresse dieselbe Telefonnummer verwendet wird; überdies können bei verschiedenen Anbietern weitere E-Mail-Accounts eröffnet werden. Ferner besteht die von der Beklagten unter Verweis auf eine Liste des Portals CHIP dargelegte Möglichkeit, sogenannte Wegwerf-E-Mail-Adressen zu generieren. Auch dem substantiierten Vortrag der Beklagten, dass Zugangslinks mittels automatisierter Software, insbesondere des OpenAI Operators, ausgefüllt werden könnten, ist der Kläger nicht entgegengetreten. Nach alledem sind andere Maßnahmen, mit denen der Einsatz von Bots und die Mehrfachregistrierung wirksam verhindert werden können, nicht ersichtlich.

hh. Auch aus den übrigen Umständen ergibt sich im Streitfall keine Unfreiwilligkeit einer Einwilligung, so dass im Rahmen des - als solches nicht streitgegenständlichen - Nachweisverfahrens eine Einwilligung in die Verarbeitung biometrischer Daten wirksam erteilt werden kann. Das in Erwägungsgrund 43 der DSGVO erwähnte Ungleichgewicht besteht nicht. Insbesondere hat die Beklagte keine marktbeherrschende Stellung und die Nutzer sind auf die Leistung nicht angewiesen. Es handelt sich um eine zusätzliche Verdienstmöglichkeit, wobei es auch andere Anbieter gibt. Hinzu kommt, dass nicht jede Kopplung automatisch die Freiwilligkeit entfallen lässt. Stattdessen muss der Kopplungssituation lediglich „in größtmöglichem Umfang Rechnung getragen werden". Das bringt zum Ausdruck, dass es noch andere Faktoren gibt, die bei der Subsumtion unter den Begriff „freiwillig" zu berücksichtigen sind. Der Verantwortliche muss also im Einzelfall prüfen, ob eine Drucksituation entsteht, die die Freiheit zur Willensentschließung aufhebt (OLG Frankfurt, Urteil vom 10.07.2025 – 6 UKl 14/24 –, Rn. 40, juris). Das ist aus den oben genannten Gründen zu verneinen.

d. Ein Verstoß gegen die Auffangvorschrift des § 307 Abs. 1 S. 1 BGB ist ebenfalls nicht gegeben. Aus den im Rahmen der Erforderlichkeit genannten Gründen liegt keine unangemessene Benachteiligung der Verbraucher entgegen den Geboten von Treu und Glauben vor.

e. Aus dem vom Kläger im Rahmen der mündlichen Verhandlung angeführten Grundsatz der kundenfeindlichsten Auslegung ergibt sich ebenfalls keine Unwirksamkeit der Klausel nach § 307 Abs. 1 S. 1 BGB oder § 307 Abs. 2 Nr. 1 BGB.

Im Rahmen eines Verbandsprozesses nach § 1 UKlaG ist bei mehreren Auslegungsmöglichkeiten von der kundenfeindlichsten Auslegung auszugehen. Auszuscheiden sind nur Auslegungsmöglichkeiten, die für an solchen Geschäften typischerweise Beteiligten ernsthaft nicht in Betracht kommen (BGH NJW 2008, 360, 363 Rn. 28). Der Kläger trägt im vorliegenden Fall jedoch keine bestimmte Auslegungsmöglichkeit der angegriffenen Klausel vor, sondern er vertritt die Auffassung, dass die Klausel mangels wirksamer Einwilligung in die Verarbeitung biometrischer Daten unwirksam sei; im Rahmen der mündlichen Verhandlung hat der Kläger nur allgemein ausgeführt, dass die Klausel weitgehende Möglichkeiten biete, die Auszahlung zu verhindern. Dies ist für den Senat so nicht nachvollziehbar. Im Übrigen gilt der Grundsatz, dass eine Klausel - auch im Verbandsprozess - vor dem Hintergrund des gesamten Formularvertrags zu interpretieren ist; sie darf nicht aus einem ihre Beurteilung mit beeinflussenden Zusammenhang gerissen werden. Es sind daher auch Formularbestimmungen eines „Gesamtklauselwerks", die mit der Klausel inhaltlich zu einer Einheit verbunden sind, bei der Auslegung zu berücksichtigen (BGH, Urteil vom 10.06.2020 – VIII ZR 289/19 –, Rn. 30, juris). Da der Kläger die AGB der Beklagten nicht eingereicht hat, sondern sich auf die Wiedergabe von Teil 2 § 3 Abs. 4 der AGB beschränkt hat, ist eine zur Unwirksamkeit der Klausel führende Auslegung, etwa in dem Sinne, dass die Beklagte im Rahmen des Nachweisverfahrens biometrische Daten ohne ausdrückliche Einwilligung der Mitglieder verarbeite, nicht möglich.

3. Die Kostenentscheidung folgt aus § 91 Abs. 1 ZPO. Die Entscheidung über die vorläufige Vollstreckbarkeit beruht auf §§ 708 Nr. 11, 711, 713 ZPO.

4. Die Revision ist gemäß § 6 Abs. 2 UKlaG i.V.m. §§ 542 Abs. 1, 543 Abs. 2 ZPO nicht zuzulassen. Die Voraussetzungen für eine Zulassung der Revision liegen nicht vor. Die Rechtssache hat weder grundsätzliche Bedeutung noch erfordern die Fortbildung des Rechts oder die Sicherung einer einheitlichen Rechtsprechung eine Entscheidung des Revisionsgerichts.

Vorsitzender Richter am Oberlandesgericht	Richter am Oberlandesgericht	Richterin am Oberlandesgericht

Für die Richtigkeit der Abschrift
Hamburg, 13.05.2026

JFAng
Urkundsbeamter der Geschäftsstelle