LG München I, Endurteil v. 29.11.2022 – 33 O 14776/19

**Titel:**

## Unzulässige Speicherung von Cookies in Endgeräten von Webseitennutzern

**Normenketten:**

TTDSG § 25

UKlaG § 2 Abs. 2 S. 1 Nr. 11

**Leitsätze:**

**1. Die Regelung des § 25 TTDSG stellt ein Verbraucherschutzgesetz im Sinne von § 2 Abs. 2 S. 1 Nr. 11 UKlaG dar. (Rn. 84) (redaktioneller Leitsatz)**

**2. Es verstößt gegen § 25 TTDSG, wenn der Betreiber einer Webseite es veranlasst, dass Cookies auf dem Endgerät des Nutzers gespeichert und zum „Tracking“ des Nutzers genutzt werden, ohne eine wirksame Einwilligung der betroffenen Nutzer einzuholen. (Rn. 96) (redaktioneller Leitsatz)**

**3. Eine Einwilligung ist nicht freiwillig, wenn der Nutzer diese lediglich in vollem Umfang erteilen oder durch Betätigung der Schaltfläche „Einstellungen“ eine gesonderte Auswahl treffen, die Webseite ansonsten aber nicht nutzen kann. (Rn. 112) (redaktioneller Leitsatz)**

**Schlagwort:**

Telemedien

**Fundstellen:**

RDV 2023, 121

K & R 2023, 220

ZD 2023, 223

GRUR-RS 2022, 39300

MMR 2023, 222

LSK 2022, 39300

## Tenor

I. Die Beklagte wird verurteilt, es bei Vermeidung eines vom Gericht für jeden Fall der Zuwiderhandlung festzusetzenden Ordnungsgeldes von bis zu € 250.000,00, ersatzweise Ordnungshaft oder Ordnungshaft bis zu sechs Monaten, letztere zu vollziehen an ihrem Geschäftsführer, zu unterlassen, im Rahmen geschäftlicher Handlungen gegenüber Verbrauchern in Telemedien für die domainübergreifende Aufzeichnung und Auswertung des Nutzerverhaltens zu Analyse- und Marketingzwecken Informationen auf dem Endgerät des Nutzers zu speichern oder auf Informationen zuzugreifen, die bereits im Endgerät der Nutzer hinterlegt sind, sofern die Speicherung oder der Endgerätezugriff für den Betrieb der Website nicht unbedingt notwendig ist, ohne vor Beginn des Nutzungsvorgangs eine informierte und freiwillige Einwilligung der Nutzer für den Zugriff auf deren Endgeräte oder Endgeräteinformationen einzuholen, wenn dies geschieht wie in Anlage K 58 dargestellt.



































































































































II. Im Übrigen wird die Klage abgewiesen.

III. Die Kosten des Rechtsstreits tragen der Kläger zu ¾ und die Beklagte zu ¼.

IV. Das Urteil ist in Ziffer. I gegen Sicherheitsleistung in Höhe von 1.000.000,- Euro und wegen der Kosten gegen Sicherheitsleistung in Höhe von 110 % des jeweils zu vollstreckenden Betrages vorläufig vollstreckbar.

## Tatbestand

1
Die Parteien streiten über die Vereinbarkeit einzelner Dienste des Online-Angebots der Beklagten mit dem Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG).

2
Der Kläger ist ein eingetragener Verein zur Wahrnehmung von Verbraucherinteressen. Er ist der Dachverband aller 16 Verbraucherzentralen und 26 weiterer verbraucher- und sozialorientierter Organisationen in Deutschland. Zu seinen satzungsmäßigen Aufgaben gehört es, die Interessen der Verbraucher durch Aufklärung und Beratung wahrzunehmen. Der Kläger ist in die Liste qualifizierter Einrichtungen im Sinne von § 4 UKlaG beim Bundesamt für Justiz eingetragen.

3

Die Beklage ist Anbieterin und Betreiberin der Webseite www.focus.de. Nach unbestritten gebliebenem Vortrag der Beklagten handelt sich dabei um das größte deutsche Nachrichtenportal. Die Beklagte stellt den Nutzern die auf der Seite vorgehaltenen Inhalte kostenfrei zur Verfügung. Sie finanziert ihr Online-Angebot allein durch Werbung. Die Beklagte nutzt dabei eine Software zur Verwaltung der Nutzerpräferenzen, eine sogenannte Consent Management Platform, kurz CMP. Diese entspricht den Vorgaben eines Branchenstandards mit der Bezeichnung „IAB Transparency and Consent Framework (TCF) 2.0“. Das TCF bietet die technische Infrastruktur für Abfrage und Übermittlung der Nutzereinwilligung zwischen Publishern, Werbungstreibenden, Vermarktern, Agenturen und den jeweiligen Technologieparinern.

4
Bei Aufruf der Webseite www.focus.de erscheint die nachfolgend abgebildete erste Seite der CMP, mittels der eine Einwilligung der Nutzenden zur Anwendung von bestimmten Diensten abgefragt wird (vgl. Anlagen K 57, K 58, K 59):

5
Die von der Beklagten verwendete CMP ist dabei in mehreren Schichten aufgebaut, in denen verschiedene Dienste in Gruppen zusammengefasst werden.

6
Bei Aufruf der Website www.focus.de - und auch vor Interaktion mit der dort vorgehaltenen CMP - wird eine gewisse Zahl von Cookies auf dem Rechner des Nutzers gesetzt, wobei deren Anzahl, der Zeitpunkt der Setzung und deren Funktion zwischen den Parteien im Einzelnen umstritten ist.

7
Nach Abfrage der Nutzereinwilligung wird jedenfalls der sogenannte TC String, eine codierte Zeichenkette, durch die CMP auf dem Rechner des Nutzers gespeichert. Der TC String enthält zumindest die relevanten Informationen im Hinblick auf die Nutzereinwilligung, wobei dessen konkreter Inhalt im Einzelnen zwischen den Parteien ebenfalls umstritten ist. Er dient als Kommunikationsmittel innerhalb des „IAB TCF Frameworks“.

8
Nachdem der Kläger ursprünlich zu der zum Zeitpunkt der Klageeinreichung von der Beklagten verwendeten Datenschutzerklärung („Cookie-Banner“) und den auf der Webseite der Beklagten zu diesem Zeitpunkt genutzten Technologien vorgetragen hat (vgl. insbesondere die Klageschrift vom 23.10.2019, Bl. 1/40 d.A. sowie die Replik vom 30.06.2029, Bl. 145/222 d.A.), trug der Kläger zuletzt wie folgt vor:

9
Die Beklagte habe nach Klageeinreichung ihre Website dahingehend umgestellt, dass beim erstmaligen Aufruf der Website ein Cookie-Banner eingeblendet werde, der eine angeblich wirksame Einwilligung abfragen solle (Anlage K 57). Dieser umfasse 142 einzelne Bildschirmansichten (vgl. Gesamtausdruck Anlage K 58). Auf der ersten Schicht („Ist Layer“) befände sich bereits keine Möglichkeit für Website-Besucher, die Zustimmung abzulehnen (Anlage K 59). Es stünden lediglich die Optionen „Akzeptieren“ und „Einstellungen“ zur Verfügung sowie Verlinkungen auf die Datenschutzerklärung sowie auf das Impressum der Beklagten:

10
Auf der zweiten Schicht gebe die Beklagte an, dass mehr als 100 Anbieter Informationen aus Endgeräten der Nutzer wie z.B. „Cookie-Informationen“ (Cookie ID) und „Gerätekennungen“ zu den dem Nutzer angezeigten Verarbeitungszwecken auf dem Endgerät speicherten und abriefen (Anlage K 60):

11
Unter der Überschrift „Anbieterübersicht“ gebe die Beklagte an, dass mehr als 100 Technologieanbieter Zugriff auf Endgeräteinformationen der Website-Besucher hätten (vgl. Gesamtausdruck, Anlage K 58).

Außerdem würden bereits Schaltflächen für mehr als ein Dutzend Anbieter vorausgewählt und dem Nutzer eine Einwilligung zugeordnet, obwohl er tatsächlich keine bestätigende Handlung vorgenommen habe (Anlagen K 61, K 62).

12
Die Beklagte gebe auf der ersten Schicht der CMP lediglich unvollständig die Verarbeitungszwecke an. So würden lediglich die Verarbeitungszwecke „Informationen auf einem Gerät speichern und/oder abrufen“, „Personalisierte Anzeigen und Inhalte“, „Anzeigen- und Inhaltsmessungen, Erkenntnisse über Zielgruppen und Produktentwicklung“ sowie „Funktional, Analytik, Werbung (nicht IAB-Anbieter), Soziale Medien und strikt erforderliche Cookies“ angezeigt. Besonders invasiv in die Grundrechte der Verbraucher eingreifende Verarbeitungszwecke würden dagegen erst auf der zweiten Schicht des Cookie-Banners nach weiteren Klicks und mehrfachem Scrollen angegeben. So sei nicht nur der Aufruf der Verlinkung „Einstellungen“ auf der ersten Schicht des Cookie-Banners erforderlich. Auf der zweiten Schicht sei sodann ein Klick auf den Link „Zusatzfunktionen“ notwendig. Erst nach diesen Schritten würden die weiteren besonders eingriffsintensiven Verarbeitungszwecke eingeblendet, wie z.B. „Zusammenführen mit Offline-Datenquellen“, d.h. Nutzerdaten aus Online-Quellen mit personenbezogenen Daten aus Offline-Quellen zusammenführen; außerdem werde unter der Rubrik „Zusatzfunktionen“ auf der zweiten Schicht des Cookie-Banners der Verarbeitungszweck „Verschiedene Geräte verknüpfen“, ebenfalls durch 80 Drittanbieter auch aus Drittstaaten außerhalb der Europäischen Union angezeigt. „Verschiedene Geräte verknüpfen“ bedeute, dass personenbezogene Daten, die über verschiedene Endgeräte (Desktop PC, Laptop, Smartphone, Tablet, Smart TV etc.) eines bestimmten Nutzers gesammelt worden seien, zusammengeführt würden. Eine Zustimmung für diese - unter der Rubrik „Zusatzfunktionen“ getarnten - besonders stark in die Grundrechte eines Verbrauchers eingreifenden Zwecke sei jedoch nicht erteilt worden. Es finde sich auch keine Information zu eben diesen Verarbeitungszwecken auf der ersten Schicht des Cookie-Banners der Beklagten, auf deren Grundlage Verbraucher in der Regel ihre Nutzerentscheidung treffen würden.

13
Der Kläger führt weiter aus, in der aktualisierten Datenschutzerklärung der Beklagten fehle es an gesetzlichen Pflichtangaben in Bezug auf eingesetzte Dienstleister wie z.B. die Angabe der Rechtsgrundlage oder die geeigneten oder angemessenen Garantien für einen Drittstaatentransfer, z.B. in die USA wie es bei dem Drittanbieter Google der Fall sei (Anlage K 76). So informiere die Beklagte bereits unzutreffend über die Rechtsgrundlagen der Datenverarbeitung beim Tracking. Unter dem Gliederungspunkt „Tracking und Nutzungsanalyse“ informiere die Beklagte Website-Besucher darüber, dass kein Tracking, sprich die Aufzeichnung und Auswertung des Nutzerverhaltens, stattfinde, wenn der Nutzer keine Einwilligung erteilt habe (Anlage K 77). Dies sei tatsächlich nicht der Fall. Ferner würden unter der Rubrik „berechtigtes Interesse“ Zustimmungen suggeriert (Anlage K 78). Klicke man indes auf die Rubrik „Ihre Einwilligung“, werde für das Tracking angezeigt, dass keine Einwilligung erteilt worden sei, obwohl eine Zustimmung des Nutzers unter der Rubrik „berechtigte Interessen“ als erteilt angezeigt werde (Anlage K 79):

14
Die Nutzer würden über die einschlägige Rechtsgrundlage im Unklaren gelassen. Die „Datenschutzoptionen“ umfassten über 500 Einzelansichten.

15
Der Kläger führt weiter aus, die Beklagte binde im Quellcode ihrer Website JavaScripte, iframes, und Image-Pixel ein, die von Drittanbietern zur Verfügung gestellt werden würden, Datenverbindungen zu diesen öffneten und Tracking-Technologien auslösten. Über diese JavaScript-Tags oder iframes eines Drittanbieters (ein HTML-Element, das weitere HTML-Elemente eines Dritten in die aktuelle Seite einbinden könne) und Image-Pixel (1×1 große Bild-Pixel im Hintergrund der Website) würden clientseitig (Endgerät des Nutzers) mittels Cookies, Browser-Fingerprinting-Verfahren, Auslesen des Local- und Session Storage sowie der IndexedDB-Datenbank Zugriffe auf Endgeräteressourcen über den verwendeten Browser des Nutzers ermöglicht, die eine Nachverfolgung und Auswertung des Nutzerverhaltens auf unterschiedlichen Websites (domainübergreifend) unterschiedlicher Anbieter und sogar auf unterschiedlichen Endgeräten erlaubten. Die Beklagte greife aufgrund der genannten Technologien auf den Web-Speicher im Browser

eines jeden Website-Besuchers zu, im Konkreten im Web-Speicher des Browsers (Cookies und Endgeräte-Ressourcen wie Local- und SessionStorage und IndexedDB-Datenbanken). Dabei ermögliche die Beklagte aufgrund der Programmierung der Website, dass eine Vielzahl von Drittanbietern auf Informationen aus Endgeräten der Nutzer (z.B. die User ID, IP-Adresse, GPS-Daten und weitere Datenparameter wie Gerätekennungen und Browser-Informationen) mittels sog. HTTP-Transaktionen, sprich Drittanbieter-Server-Anfragen zugreifen bzw. Informationen in Endgeräten ablegen und auslesen könnten. Der Kläger verweist im Übrigen auf seine Ausführungen in der Replik vom 30.06.2020 (Bl. 145/222 d.A.). Auf diese und die dortigen Anlagen wird auch im Rahmen des Tatbestands vollumfänglich Bezug genommen.

16
Weiter führt der Kläger aus, es sei im Rahmen einer Echtzeitanalyse der Netzwerkverbindungen (HTTP-Transaktionen) der Website der Beklagten mit Internet-Domänen am 05.01.2021 festgestellt worden, dass die Beklagte JavaScripte und iframes im Quellcode ihrer Website implementiert habe, die von Drittanbietern zur Verfügung gestellt würden und daher unter ihrer Domäne (www.focus.de) aufgrund von First Party-Cookies, Third-Party-Cookies und der Nutzung LocalStorage, SessionStorage und IndexedDB Endgeräteinformationen im Webspeicher des Browsers von Nutzern speichere oder auf Endgeräteinformationen zugreife. Die Echtzeitanalyse sei mithilfe der Konsole für Webentwickler des Standard-Browsers Firefox (Version 83.0, 64 Bit) mit einem handelsüblichen Desktop PC (Windows 10) vom Standort Leipzig durchgeführt worden. Der Browser sei zuvor bereinigt worden, indem vor Aufruf der Website der Beklagten alle Cookies und Website-Daten entfernt worden seien, die den Cache des Browsers belegt hätten (vgl. Teil-Ausdrucke Webspeicher des Browsers, Anlagen K 63, K 64, K 65). Ohne dass ein Nutzer mit dem Cookie-Banner der Beklagten interagiert habe, würden bereits neben knapp einem Dutzend anderer First-Party-Cookies auch Google Analytics Cookies mit der Bezeichnung „_gat_UA-89731071-12“, „_ga“ und „gid“, die über frei zugängliche Tracker-Datenbanken unter www.better.fyi und www.whotracks.me eindeutig den Webservern von Google zugeordnet werden könnten, unter der Domäne „www.focus.de“ im Webspeicher des Browsers des Nutzers hinterlegt werden (Anlage K 66). Ebenso erfolgten ohne jedwede Interaktion mit dem Cookie-Banner ein Zugriff auf und eine Speicherung von Informationen aus Endgeräten über den Web-Speicher LocalStorage und den SessionStorage des Browsers des Nutzers (Anlage K 67).

17
Die User ID (Cookie ID) - eine einmalig vergebene und dem Website-Besucher zugewiesene Nummer - werde in den Cookies im Web-Speicher des Browsers im Endgerät gespeichert und stelle eine Endgeräteinformation dar. Bei jedem weiteren Aufruf der Website der Beklagten würden aufgrund der Cookies Endgerätezugriffe auf die IP-Adresse und User ID des Nutzers sowie auf folgende Informationen durch Drittanbieter ermöglicht werden:

- Nutzerverhalten (Interaktionen, festgelegte Ereignisse wie Aufruf einer bestimmten Seite),

- besuchte Webseiten/Umfelder, Browserinformationen, Standort-Informationen, Systemdaten,

- Geräteinformationen (z.B. Betriebssystem, Grafikkarte etc.), Views, Profildaten, UserAgent, IPAdresse,

- Mobile Identifier (Gerätetyp etc.), ggf. Mobile Werbe IDs (IDFA/GAID),

- Browser Informationen: CSS-Informationen; JavaScript-Objekte (z.B. Dokument, Fenster, Bildschirm, Browser, Datum und Sprache); HTTP-Kopfdaten (z.B. Zahl der Informationsbits in der Benutzeragenten-Zeichenfolge (User-Agent-String), Abfolge im HTTPHeader, Variationen des HTTP-Headers je nach Art der Abfrage); Uhrzeitinformationen (z.B. Uhrabweichung und Zeitfehler); Variation des TCP-Stapels installierte Schriftarten;

- Informationen zu installierten Plug-ins (z.B. Angaben zu Konfiguration und Version);

- Verwendung interner Programmierschnittstellen (API/SDK), die über den Benutzeragenten/das Gerät zugänglich seien;

- Verwendung externer API von Webdiensten, mit denen der User Agent/das Gerät kommuniziere.

18
Im Rahmen der Echtzeitanalyse habe ferner beobachtet werden können, dass allein beim Aufruf der Startseite der Website www.focus.de und ohne Interaktion mit dem Cookie-Banner 40 HTTP Anfragen an 13 unterschiedliche Domains von Drittparteien versendet werden würden, sodass die Drittanbieter auf Endgeräteinformationen zugreifen könnten. Diese Drittparteien ließen sich Firmengruppen zuordnen (Anlage K 69). Die genaue Unternehmensbezeichnung könne der „Anbieterübersicht“ auf der zweiten Schicht des Cookie-Banners entnommen werden (vgl. Gesamtausdruck des Cookie-Banners, Anlage K 58). Diese Transaktionen ermöglichten es den Drittparteien, vielfältige Informationen über den Nutzer in Erfahrung zu bringen sowie den Nutzer mit individuellen Identifikationscodes (User ID/Cookie ID) zu markieren und später wiederzuerkennen - sowohl beim erneuten Besuch auf der Website www.focus.de als auch bei Besuchen auf anderen Websites. Zudem würden manche dieser Drittparteien versuchen, den Browser des Nutzers mit bestehenden digitalen Profilen aus anderen Quellen zu verknüpfen - über Plattformen, Geräte und Lebensbereiche hinweg. Die Transaktionen fänden im Kontext des Nutzer-Browsers statt, würden jedoch durch den Abruf von www.focus.de initiiert werden (Anlage K 69).

19
Ferner behauptet der Kläger, dass nach einer vermeintlichen Zustimmung der Nutzer First-Party-Cookies sowie Third-Party-Cookies von mindestens 18 fremden Domänen im Webspeicher des Browsers von Nutzern nebst User ID von der Beklagten gespeichert würden. Bei weiteren Aufrufen de: Website der Beklagten erfolge ein Zugriff auf Endgeräteinformationen wie die IP-Adresse und User ID (Cookie ID) durch Drittanbieter (vgl. Teilausdruck des Web-Speichers im Browser, Anlage K 63). Die Beklagte löse darüber hinaus Zugriffe auf und Speicherungen von Endgeräteinformationen an über 18 fremde Domänen im Webspeicher des Browsers über den LocalStorage aus (vgl. Anlage K 64). Schließlich löse die Beklagte darüber hinaus Zugriffe auf und Speicherungen von Endgeräteinformationen an über 18 fremde Domänen im Webspeicher des Browsers über den SessionStorage aus (vgl. Anlage K 65).

20
Selbst in dem Fall, in dem der Nutzer ein Tracking mittels Cookies und ähnlichen Technologien ausdrücklich ablehne, würden bereits neben knapp einem Dutzend anderer First-Party-Cookies auch Google Analytics Cookies mit der Bezeichnung „_gat_UA-89731071-12“, „_ga“ und „gid“, die über frei zugängliche Tracker-Datenbanken unter www.better.fyi und www.whotracks.me eindeutig den Webservern von Google zugeordnet werden könnten, unter der Domäne „www.focus.de“ im Webspeicher des Browsers des Nutzers hinterlegt werden (Anlage K 71). Allein beim Aufruf der Startseite der Website www.focus.de würden im Fall der Ablehnung einer Zustimmung auf dem Cookie-Banner 142 HTTP-Anfragen an 31 unterschiedliche Domains von Drittparteien versendet werden, sodass die Drittanbieter auf Endgeräteinformationen zugreifen könnten (vgl. Anlage K 74). Daneben würden Third-Party-Cookies des Werbenetzwerkes Criteo im Webspeicher des Browsers des Nutzers abgelegt werden. Bei weiteren Aufrufen der Website der Beklagten würden etwa die User ID (Cookie ID) von Criteo als Werte der Cookies neben der IP-Adresse an den Webserver von Criteo mit der Domäne www.gum.criteo.com übermittelt werden (vgl. Anlage K 71). Bei diesen Cookies handele es sich um persistente Cookies, die eine Nachverfolgung von Nutzern über einen ausgedehnten Zeitraum von mehreren Monaten und Jahren ermöglichten. So werde z.B. der Google Analytics-Cookie „_ga“ auf den Endgeräten der Nutzer gespeichert und ermögliche bei jedem Aufruf der Website der Beklagten die streitgegenständliche Datenübermittlung an Google und damit eine fortlaufende Profilbildung (vgl. Anlage K 71). Aufgrund der Einstellung zum „Cross-Domain-Tracking“ im Google Analytics-Account würden Nutzer über mehrere Websites hinweg verfolgt werden. Diese Funktion biete Google auch für das Tracking von Nutzern mittels First-Party-Cookies an. Würden die gleichen Tracking-Codes auf beiden Websites eingebaut, könnten die Besucher auf den beiden Websites durch denselben Nutzer zu einem einzigen Besuch zusammengefügt werden. Um das Nutzungsverhalten websiteübergreifend nachzuverfolgen, müsse der Tracking-Code lediglich die Besuchererkennung aus einem URL-Parameter übernehmen: Auf der ersten Website werde die Besuchererkennung aus dem First-Party-Cookie ausgelesen und alle Links, die zur zweiten Website führten, als URL-Parameter angehängt und um den Zeitstempel des Besuchs ergänzt. Auf der zweiten Website erkenne der Tracking-Code die angehängte Besuchererkennung und übernehme diese für das Tracking-Cookie. Das Javascript von Google „analytics.js“, welches auch im Quellcode der Website der Beklagten implementiert sei, müsse dafür lediglich um die Funktion „linker“ ergänzt werden. Die Beklagte habe das JavaScript zur Erweiterung von

Google Analytics (Universal Analytics) „linkid.js“ zum domänenübergreifenden Tracking auch im Quellcode ihrer Webseite implementiert. Aufgrund dieses JavaScripts erfolge eine Serveranfrage auf jeder aufgerufenen Webseite, die einem First-Party-Cookie zugeschrieben werde und ermögliche deshalb eine domänen- und websiteübergreifende Nachverfolgung (Anlage K 84). Die Beklagte habe daneben u.a. den Tracking-Programmcode „Google AMP Client ID“ mit dem Zweck eines domainübergreifenden Trackings auf ihrer Seite eingebunden und konfiguriert.

21
Der Kläger behauptet ferner, es erfolge auch nach expliziter Ablehnung einer Einwilligung auf der zweiten Schicht des Cookie Banners ein Zugriff auf und eine Speicherung von Informationen aus Endgeräten über den Web-Speicher LocalStorage und des SessionStorage des Browsers des Nutzers.

22
Der Kläger trägt weiter vor, die Beklagte bediene sich bei der Vermietung von Werbeflächen der Funktion des sogenannten „Real Time Biddings“, mit der Werbeflächen auf der Webseite der Beklagten in Echtzeit an den höchstbietenden Werbetreibenden über die Werbenetzwerke von Google und Criteo automatisiert versteigert werden würden. Dabei würden die zuvor gesammelten Profilinformationen der Website-Besucher faktisch mitversteigert. Das Skript für das „Real-Time-Bidding“-System „Authorized Buyers“ („Double Click AdExchange“) mit dem Namen „https://securepubads.g.doubleclick.net/gpt/pubad…01.js“ mit der Domain https://pagead2.googlesyndication.com von Google sei in dem Quellcode der Website der Beklagten implementiert (Anlage K 9). Die gesammelten Informationen der Website-Besucher der Beklagten würden in eine „Gebotsanfrage“ („Bid-Request“) aufgenommen, wenn ein Nutzer die Website der Beklagten besuche. Diese Informationen würden in das „Real-Time-Bidding“-Ökosystem, wie es von Google (Double Click/Authorized Buyers) bereitgestellt werde, übertragen, sodass Werbetreibende auf passende Werbeanzeigen bieten könnten. Die Gebotsanfragen würden mithilfe von Cookies und ähnliche Technologien der Drittanbieter ermöglicht und enthielten personenbezogene Daten der Website-Besucher. Die Erfassung der Informationen der Website-Besucher, die Erstellung der Gebotsanfrage, die Versteigerung, das Bieten und Sichern der Werbefläche und die anschließende Präsentation der Werbung bei dem Website-Besucher erfolgten in Millisekunden. Dies ermögliche es dem meistbietenden Werbetreibenden, Einzelpersonen Anzeigen auf der Grundlage der über den Real-Time-Bidding-Prozess gesammelten Informationen zu präsentieren.

23
Mit jeder von der Beklagten ausgelösten Gebotsanfrage werde auch eine Kennung an Dritte versendet, die Consent String genannt werde. Bei dem Consent String handele es sich um eine eindeutige Kennung einer Person, die aufzeichne, welche Websites und Apps von ihr verwendet würden. Folgende Daten seien im Consent String enthalten:

- eine ständige Aufzeichnung des exakten Zeitpunkts (bis auf eine Zehntelsekunde) und des Datums, zu dem der TCF Consent String über die betreffende Person erstmalig erstellt worden sei (dieser Zeitstempel sei mit hoher Wahrscheinlichkeit für jedes Individuum einzigartig);

- die Sprache der Person;

- das Land, in dem die betrachtete Website gehostet werde; die Optionen, die die Person in den TCF Consent & Transparency Notices ausgewählt habe;

- die Version der Consent Management Plattform;

- der exakte Zeitpunkt (bis auf eine Zehntelsekunde) und das Datum, zu dem die Aufzeichnung das letzte Mal geändert worden sei. Dies ermögliche jedem, der Zugang zu dem Consent String habe, neue Daten über die Person zu ergänzen.

24
Die endgerätebezogenen Informationen über den Nutzer in der Gebotsanfrage umfassten folgende Angaben von Nutzern: Zielgruppen-/Targeting IDs und die darin enthaltenen User-Matching IDs, IPAdresse, User ID, Standort-Informationen, Geo-ID, GPS-Daten, Browser-Informationen, Geräteinformationen (z.B.

Betriebssystem und App-Name) sowie Mobile Werbe IDs (IDFA/GAID) beim Aufruf mit einem Smartphone, Tablet oder SmartTV).

25
Der Kläger führt hierzu weiter aus, dass am 15.11.2021 um ca. 17:14 Uhr aufgrund der Integration der Tracking-Codes auf der Website der Beklagten www.fokus.de im Rahmen einer Echtzeitanalyse mit einem handelsüblichen Desktop-PC (Windows 10, Browser: Chrome v95.0) beim Laden der URL im Hintergrund vom Browser des Klägers zwei Serveranfragen (https://ib.adnxs.com/ut/v3) zur Abgabe einer Gebotsanfrage ausgesendet worden seien. Mit diesen Serveranfragen der Beklagten sei die Xandr, Inc. - als der von der Beklagten eingesetzte Ad „Exchange-Anbieter“ (Online-Werbebörse) - aufgefordert worden, Gebotsanfragen an die Vielzahl von Unternehmen, die an ihren Auktionen teilnähmen, zu senden. Dabei werde mittels Cookies („Set-Cookie“) unter dem Namen „uuid2“ von Xandr. auf Endgerätinformationen zugegriffen (vgl. Anlage K 81).

26
Die von der Beklagten am 15.11.2021 um 17:14 Uhr initiierte Serveranfrage (https://ib.adnxs.com/ut/v3) zur Aufforderung der Abgabe einer Gebotsanfrage durch die Xandr Inc. habe alle für die Durchführung einer Real Time Bidding-Auktion erforderlichen Datenparameter des Klägers wie die User ID („uuid2“), Cookie-Informationen zum Abgleich mit Drittanbieter-Plattformen (Matching ID), Angaben zu Browser-Einstellungen von Nutzern, Parameter für die Auktion sowie Serverinformationen enthalten. Die Serverantworten der Xandr Inc. auf die von der Beklagten initiierte Serveranfrage (https://ib.adnxs.com/ut) enthielten mehrfach klare Referenzen auf Real Time Bidding („content_source“: „rtb“, „rtb_video_fallback“, „rtb“, „banner“) und Angaben zur Auktion („AuctionsID“, „Buyer-Member ID“, d.h. Gewinner der Auktion), Creative-ID, zum gezahlten Entgelt (CMP = Cost per Mile), sowie zur gezahlten Währung („publisher_currency_code“, „€“), vgl. Anlage K 82.

27
Daneben habe die Beklagte die Funktion „Push Pages“ von Google implementiert, durch die Google während des „Real-Time-Bidding“-Prozesses mehrere Unternehmen einlade, weitere Profilbezeichnungen über eine Person auszutauschen, wenn sie eine Webseite laden würden. Die Beklagte habe das entsprechende Google-Skript auf ihrer Website implementiert und wirke an dem Datenaustausch auch über die Google Domain für die Funktion Push-Pages (https://pagead2.googlesyndication.com) mit (Anlage K 9). Google Push Pages würden von einer Google-Domain (https://pagead2.googlesyndication.com) aus bedient und hätten alle den gleichen Namen, „cookie_push.html“. Jede Push-Seite sei durch einen Code von fast zweitausend Zeichen gekennzeichnet, den Google am Ende hinzufüge, um die Person, über die Google Informationen weitergebe, eindeutig zu identifizieren. Dies, in Kombination mit anderen von Google bereitgestellten Cookies, ermögliche es Unternehmen, die Person pseudonym zu identifizieren, wenn dies sonst nicht möglich wäre. Alle Unternehmen, die von Google zum Zugriff auf eine Push Page eingeladen werden würden, erhielten die gleiche Kennung für die zu profilierende Person. Dieser „google_push“-Identifikator ermögliche es ihnen, ihre Profile der Person zu vergleichen und sie könnten dann Profildaten miteinander austauschen (vgl. Anlage K 13).

28
Der Kläger ist der Auffassung,

er sei klagebefugt. Der Europäische Gerichtshof habe mit Urteil vom 28.04.2022 (C-319/20 - App Zentrum = ZD 2022, 384 ff.) die Klagebefugnis des Klägers sowohl nach UKlaG als auch nach UWG bejaht.

29
Der Kläger meint, sämtliche von der Beklagten genutzten Tracking Technologien würden einem Einwilligungsvorbehalt unterliegen. Die Nutzung dieser Technologien ohne informierte und freiwillige Entscheidung des Nutzers sei daher rechtswidrig. Dies sei nach der EuGH-Entscheidung „Planet49“ zwischenzeitlich auch vom BGH mit Urteil vom 28.05.2020 (Az.: I ZR 7/16 - „Cookie-Einwilligung II“) bestätigt worden. Vorliegend finde aber eine Speicherung von und ein Zugriff auf Informationen aus Endgeräten durch die Beklagte und Drittanbieter zur domainübergreifenden Aufzeichnung und Auswertung des Nutzerverhaltens zu Analyse- und Marketingzwecken bereits dann statt, wenn der Nutzer entweder nicht mit dem Cookie-Banner der Beklagten interagiere oder explizit eine Zustimmung ablehne.

30

Im Übrigen sei der von der Beklagten vorgehaltene Einwilligungsmechanismus unwirksam, weil

- es an der Freiwilligkeit der Einwilligung fehle,

- keine Einwilligung „für den bestimmten Fall“ i.S.d. Art. 4 Nr. 1 DSGVO gegeben sei;

- keine unmissverständlich abgegebene Willensbekundung vorliege. Die von der Beklagten gewählte Gestaltung sei eine faktische Voreinstellung des Einverständnisses.

31
So sei der von der Beklagten genutzte Standard „Transparency and Consent Framework (v2.0)“ der IAB Europe (TCF) von der belgischen Datenschutzaufsichtsbehörde (Autorité de protection des donnée - Gegevensbeschermingsautoriteit, „APD-GBA“) für rechtswidrig erklärt und die Löschung der auf Basis dieses „Frameworks“ gewonnenen Daten angeordnet worden (vgl. APD-GBA, Decision on the merits 21/2022 of 2 February 2022, Case number; DOS-2019-01377, abrufbar in englischer Sprache unter: https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf#page111). Mit Verfügung vom Februar 2022 sei gegenüber der für den Standard mitverantwortlichen IAB Europe entschieden worden, dass Verarbeitungen mittels des TC-Consent-Strings gegen grundlegende Pflichten aus der DSGVO verstießen, insbesondere aufgrund der Komplexität der Verarbeitung nicht den Transparenzforderungen entsprächen, und entsprechende Verarbeitungen deshalb rechtswidrig seien.

32
Die APD-GBA habe entschieden,

- dass der TC-String die Kriterien von Art. 4 Abs. 1 DSGVO erfülle und damit ein personenbezogenes Datum darstellt;

- alle an TCF teilnehmenden Organisationen als Joint Controller nach Art. 26 DSGVO für die durchgeführten Verarbeitungen des TC-Strings sowie der auf Basis des TC-Strings übermittelten personenbezogenen Daten verantwortlich seien,

- und damit gesamtschuldnerisch nach Art. 26 Abs. 3 DSGVO haften würden sowie

- dass der TCF-Standard aufgrund der Komplexität der Verarbeitungen nicht mit den Transparenzforderungen der DSGVO in Einklang stehe.

33
Aufgrund der Abfrage einer Zustimmung und die gleichzeitige Berufung der Beklagten auf „berechtigte Interessen“ in Bezug auf ein und dieselben Tracking-Dienste liege auch eine Irreführung über die Rechte der Verbraucher nach § 5 Abs. 1 Nr. 7 UWG vor. Außerdem folge die Irreführung der Verbraucher bereits aus der Einholung einer unzureichenden Einwilligung.

34
§ 2 Abs. 1 S. 2 UKlaG erweitere den Adressatenkreis von Unterlassungsansprüchen bei der Zuwiderhandlung gegen Verbraucherschutzgesetze wie die DSGVO auf Mitarbeiter und Beauftragte. Vor dem Hintergrund der Entscheidung BGH GRUR 2009, 1167 ff. - Partnerprogramm sei ein Unterlassungsanspruch gegenüber der Beklagten nach § 2 Abs. 1, Abs. 2 Nr. 11 UKlaG sowie nach § 8 UWG bereits deshalb begründet, weil die von der Beklagten eingeschalteten Dritten selbst rechtswidrig handelten, denn die Beklagte habe diese Dritten zur Erweiterung ihrer Geschäftstätigkeit eingesetzt und die Ergebnisse der Datenverarbeitung dieser Dritten kämen der Beklagten zugute.

35
Der Kläger meint, die Beweislast für die Einhaltung der DSGVO liege bei der Beklagten als Verantwortliche. Denn aufgrund der ausdrücklichen Verweisung in § 25 Abs. 1 S. 2 TTDSG auf die Modalitäten der Einwilligung nach der DSGVO als lex generalis unterlägen Datenverarbeitungen nach TTDSG dem Rechenschaftsprinzip von Art. 5 Abs. 2 DSGVO. Demnach trage die Beklagte die volle Beweislast für die

Rechtmäßigkeit ihrer Datenverarbeitung. Die Beklagte trage als Verantwortliche für das Setzen, Auslesen von bzw. Zugreifen auf Cookies sowie für andere Tracking-Technologien, die personenbezogene Daten an Dritte übermittelten, aufgrund der gesetzlich normierten Nachweispflichten die Darlegungs- und Beweislast in Bezug auf die gerügten Normen. Aufgrund der Rechtsfolgenverweisung gemäß Art. 5 Abs. 3 S. 1 ePrivacy-RL für die Anforderungen an eine wirksame Einwilligung sei somit nach wie vor auf die Beweislastregel in Art. 7 Abs. 1 DSGVO abzustellen. Im Übrigen werde die Beweislast für die Beklagte als (gemeinsam) Verantwortliche explizit in der Überschrift von Erwägungsgrund 42 DSGVO „Beweislast und Erfordernisse einer Einwilligung“ betont. Es sei für die Beklagte auch ohne Weiteres möglich, darzulegen und zu beweisen, dass keine Endgeräteinformationen von Website-Besuchern (Nutzern) zu Analyse- und Werbezwecken erfasst würden. Denn der Endgerätezugriff auf GPS-Daten, IP-Adressen, Cookie ID (User ID), Geräte und Browserinformationen des jeweiligen Nutzers durch die benannten Drittanbieter erfolge nur, weil die Beklagte aktiv und eigenständig Tracking-Codes und andere von den Drittanbietern bereitgestellte Tracking-Technologien in ihre Website einfüge. Es handele sich dabei um tatsächliche Umstände, die dem Einblick des Klägers entzogen seien. Nur die Beklagte wisse, welche Tracking-Codes von welchen Drittanbietern sie selbst in den Quellcode ihrer Website eingefügt habe.

36
Informationen über das Wesentliche einer Vereinbarung über die gemeinsame Verantwortlichkeit für die streitgegenständliche Verarbeitung i.S.d. Art. 26 Abs. 2 S. 2 DSGVO seien weder in der „Datenschutzerklärung“ noch in den dort verlinkten „Datenschutzoptionen“ zu finden (vgl. Anlage K 80). Es liege eine gemeinsame Verantwortlichkeit nach Art. 26 Abs. 1 S. 1 DSGVO vor, für die die besonderen Informationspflichten aus Art. 26 Abs. 2 S. 2 DSGVO zu erfüllen seien. Es liege eine gemeinsame Verantwortlichkeit zwischen einem Website-Betreiber und Tracking-Anbieter vor, wenn der Website-Betreiber den vom Tracking-Anbieter zur Verfügung gestellten Tracking Code (z.B. Image-Pixel, JavaScript oder iFrame) aktiv und eigenständig in seinen Quellcode der Website implementiere. Bereits die Ermöglichung, dass ein Dritter Cookies auf Endgeräten von Nutzern setze, begründe eine gemeinsame Verantwortlichkeit.

37
Der Kläger hat ursprünglich von der Beklagten Unterlassung begehrt, gegenüber Verbrauchern in Telemedien für das Tracking von Nutzern zu Analyse- und Marketingzwecken Technologien einzusetzen, die personenbezogene Daten von Nutzern an Dritte übermitteln und dadurch das Verhalten von Nutzern websiteübergreifend nachverfolgen, ohne vor Beginn des Nutzungsvorgangs eine informierte und freiwillige Einwilligung der Nutzer für diese Verarbeitung einzuholen, wenn dies geschieht, wie in Anlagen K 14 und K 15 dargestellt und gegenüber Verbrauchern Telemedien anzubieten, ohne Nutzern zu Beginn des Nutzungsvorgangs Informationen, die sich auf die Verarbeitung personenbezogener Daten nach Antrag zu 1) beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln, wenn dies geschieht, wie in Anlagen K 15 - K 21 dargestellt sowie im Falle gemeinsamer Verantwortlichkeit für die Verarbeitung personenbezogener Daten entgegen Art. 26 Abs. 2 S. 2 DSGVO das Wesentliche der Vereinbarung zwischen den gemeinsam für die Verarbeitung Verantwortlichen den Nutzern nicht zur Verfügung zu stellen, wenn dies geschieht, wie in Anlage K 21 dargestellt.

38
Der Kläger hat mit Schriftsätzen vom 25.09.2020 (Bl. 253/264 d.A.) und vom 11.01.2021 (Bl. 298/366 d.A.) die Klageanträge abgeändert und in der mündlichen Verhandlung am 23.11.2021 zudem den ursprünglich gestellten Antrag auf Kostenerstattung zurückgenommen.

39
Nachdem der Kläger die ursprünglich angekündigten Klageanträge auf Verstöße gegen die Datenschutzgrundverordnung gestützt hat (vgl. Schriftsatz vom 23.09.2020, Bl. 253/264 d.A.), hat er zuletzt in der mündlichen Verhandlung vom 12.07.2022 klargestellt, dass die zwischenzeitlich geänderten Klageanträge nunmehr ausschließlich auf § 25 TTDSG gestützt werden würden (vgl. Bl. 632 d.A.).

40
Der Kläger beantragt zuletzt:

Die Beklagte wird verurteilt, es bei Vermeidung eines vom Gericht für den Fall der Zuwiderhandlung festzusetzenden Ordnungsgeldes - ersatzweise Ordnungshaft- oder einer Ordnungshaft bis zu sechs

Monaten, (Ordnungsgeld im Einzelfall höchstens 250.000,00 EUR, Ordnungshaft insgesamt höchstens zwei Jahre), zu vollziehen an ihrem gesetzlichen Vertreter, zu unterlassen, im Rahmen geschäftlicher Handlungen gegenüber Verbrauchern in Telemedien für die domainübergreifende Aufzeichnung und Auswertung des Nutzerverhaltens zu Analyse- und Marketingzwecken Informationen auf dem Endgerät des Nutzers zu speichern oder auf Informationen zuzugreifen, die bereits im Endgerät der Nutzer hinterlegt sind, sofern die Speicherung oder der Endgerätezugriff für den Betrieb der Website nicht unbedingt notwendig ist,

1. ohne vor Beginn des Nutzungsvorgangs eine informierte und freiwillige Einwilligung der Nutzer für den Zugriff auf deren Endgeräte oder Endgeräteinformationen einzuholen, wenn dies geschieht wie in Anlage K 58 dargestellt.

2. ohne den Nutzern zu Beginn des Nutzungsvorgangs Informationen über die Speicherung von Informationen oder über den Zugriff auf Informationen, die bereits im Endgerät der Nutzer hinterlegt sind, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln, wenn dies geschieht wie in Anlagen K 76 und K 80 dargestellt.

3. im Falle gemeinsamer Verantwortlichkeit für die Speicherung von Informationen oder für den Zugriff auf Informationen, die bereits im Endgerät der Nutzer hinterlegt sind, entgegen Art. 26 Abs. 2 S. 2 DSGVO das Wesentliche der Vereinbarung zwischen gemeinsam für die Verarbeitung Verantwortlichen den Nutzern nicht zur Verfügung zu stellen, wenn dies geschieht wie in Anlagen K 76 und K 80 dargestellt.

41
Die Beklagte beantragt:

Klageabweisung.

42
Vorsorglich beantragt die Beklagte ferner (Bl. 496/499 d.A.), die Höhe einer etwaigen Sicherheit gem. § 709 S. 1 ZPO auf nicht unter eine Millionen Euro festzusetzen und der Beklagten nachzulassen, die Vollstreckung durch Sicherheitsleistung oder Hinterlegung ohne Rücksicht auf eine Sicherheitsleistung des Gläubigers abzuwenden, § 712 Abs. 1 S. 1 ZPO.

43
Die Beklagte trägt vor,

sie stelle mit der CMP ihren Nutzern eine Plattform zur Verwaltung ihrer Präferenzen zur Verfügung, die nach dem Branchenstandard TCF 2.0 zertifiziert sei. Die hiergegen gerichteten Angriffe des Klägers seien unberechtigt. Die Aussage des Klägers, wonach der „vollständige Cookie-Banner“ auf der Website der Beklagten 142 einzelne Bildschirmansichten umfasse, sei irreführend. Es sei keineswegs so, dass die Nutzer 142 Bildschirmansichten zur Kenntnis nehmen müssten, um ihre Präferenzen einstellen zu können. Die CMP sei vielmehr nach dem allgemein anerkannten „layered approach“ so aufgebaut, dass die verschiedenen Dienste zu Gruppen zusammengefasst seien und lange Listen von Dienstleistem/Vendoren nur derjenige Nutzer durchscrollen müsse, der eine differenzierte Einzelentscheidung über die Zulassung treffen wolle. Es liege auf der Hand, dass dies nur sehr wenige seien. Bereits auf der ersten Ebene befände sich die explizite Angabe „Unter ‚Einstellungen‘ können Sie Ihre Einstellungen ändern oder die Datenverarbeitung ablehnen.“ Daher wüssten die Nutzer unmittelbar, dass unter „Einstellungen“ auch eine vollständige Ablehnung möglich sei. Wer davon Gebrauch machen wolle, könne ganz einfach auf „Einstellungen“ klicken. Weder die DSGVO noch die ePrivacy-Richtlinie enthielten eine Regelung dahingehend, dass ein „Ablehnen“ schon auf der ersten Ebene der CMP mittels eines eigenen Buttons möglich sein müsse. Einen entsprechenden Regelungsvorschlag des Bundesrats im Gesetzgebungsverfahrens für ein TTDSG (vgl. BT-Drs. 19/28396 S. 6) habe die Bundesregierung in ihrer Gegenäußerung abgelehnt Diese Zweistufigkeit sei inzwischen von den Internetnutzern „gelernt“. Mitnichten hätten auch alle aufgelisteten Technologieanbieter Zugriff auf Endgeräteinformationen der Website-Besucher. Vielmehr handele es sich hierbei nur um eine Auflistung derjenigen Anbieter, mit denen die Beklagte direkt oder indirekt zusammenarbeite und die daher potenziell Technologien auf der Website der Beklagten einsetzten. Bei jedem Seitenbesuch finde ein tatsächlicher Zugriff nur durch einen kleinen Teil der Anbieter statt. Dies werde in den bereitgestellten FAQs (vgl. Anlage B 17) ausführlich erklärt. Die Formulierung des Klägers, die aufgelisteten Technologieanbieter erhielten Zugriff auf

„Endgeräteinformationen“ der Website-Besucher, erscheine ebenfalls irreführend. Es sei bei weitem nicht so, dass jeder Anbieter auf „alle möglichen“ Informationen zugreifen könne, die auf dem Endgerät des Nutzers gespeichert seien. Im Wesentlichen gehe es darum, dass der betreffende Anbieter auf ein von ihm selbst auf dem Nutzerrechner gesetztes Cookie oder - soweit vorhanden - eine Geräte-ID zugreifen könne. Dies ermögliche dem Anbieter ggf. eine Wiedererkennung - und kein Ausspionieren - des betreffenden Geräts. Die Behauptung des Klägers, in der „Anbieterübersicht“ (Anlage K 61) seien die Schaltflächen für mehr als ein Dutzend Anbieter vorausgewählt und dem Nutzer werde eine Einwilligung zugeordnet, obwohl er tatsächlich keine bestätigende Handlung vorgenommen habe, sei unwahr. In der von der Beklagten verwendeten CMP werde keinem Nutzer eine Einwilligung zugeordnet, obwohl er tatsächlich keine bestätigende Handlung vorgenommen habe. Die „Anbieterübersicht“ zeige nicht die erteilten Einwilligungen an, sondern alle über die CMP verwalteten Befugnisse. Dazu gehöre auch die Verarbeitung von Daten aufgrund berechtigter Interessen. Diese könne aktiv sein, ohne dass der Nutzer eingewilligt habe. Der Schieber stehe dann in der Regel auf einer Mittelstellung und zeige die Farbe gelb, um anzuzeigen, dass hier eine Entscheidung des Nutzers in Richtung „alles erlauben“ (= Einwilligung) ebenso möglich sei wie in Richtung „alles verbieten“ (= Widerspruch gegen Verarbeitung auf Basis berechtigten Interesses). Stehe der Schieber schon rechts (blau = alles erlaubt), dann liege dies daran, dass der betreffende Anbieter überhaupt keine einwilligungspflichtigen Handlungen vornehme.

44
Zum Hintergrund des TC String führt die Beklagte aus, dass - nachdem der „Consent“ abgefragt worden sei - sichergestellt werden müsse, dass Publisher, Werbetreibende und jede der angeschlossenen Technologieplattformen die Wünsche des Nutzers respektierten. Dazu diene der IAB TC String. Dieser werde durch die CMP auf dem Rechner des Nutzers gespeichert und bei erneutem Aufruf der Seite an sämtliche Anbieter in der Advertising-Wertschöpfungskette weitergereicht. Damit diene er als Kommunikationsmittel innerhalb des IAB TCF Frameworks. Das TCF biete eine technische Standard-Infrastruktur für die Abfrage und Übermittlung der Nutzereinwilligung zwischen Publishem, Werbungtreibenden, Vermarktern, Agenturen und ihren jeweiligen Technologiepartnern. Ziel dieses Frameworks sei es, zu standardisieren, wie Unternehmen weiterhin programmatische Werbung ausspielen könnten, ohne dabei gegen die DSGVO oder ePrivacy-Anforderungen zu verstoßen. Deshalb habe das IAB Europe als Betreiber des TCF eine Reihe von Standardzwecken definiert und führe eine Liste der registrierten Drittanbieter (sogenannte „Vendoren“) wie auch eine Liste der registrierten CMPs. Die Registrierung als Vendor erfolge über ein Bewerbungsverfahren. Diese müssten dabei die Zwecke der Datenverarbeitung und weitere Merkmale angeben. Diese müssten dabei auch den Link zu ihrer Datenschutzerklärung hinterlegen, welche wiederum DSGVO-konform sein müsse. CMPs müssten einen Validationstest durchlaufen, bevor ihnen ermöglicht werde, innerhalb des TCF anerkannte Einwilligungssignale durch den TC String zu setzen. Alle Beteiligten an dieser komplexen Struktur müssten sich zur Einhaltung der TCF Policies verpflichten. Dadurch seien u.a. die Formulierungen der möglichen Nutzereinwilligungen in Gestalt einzelner „Purposes“ (Zwecke) oder „Stacks“ (Zusammenfassungen mehrerer Zwecke) vorgegeben. Kein einzelner Beteiligter könne Änderungen an den vorgegebenen Abläufen oder Einwilligungsformulierungen vornehmen, ohne die wechselseitige Kommunikation und Anerkennung der Signale zu zerstören. Das Layout einer CMP, insbesondere deren Einteilung in unterschiedliche „Layer“, werde durch den CMP-Anbieter bestimmt.

45
Der Consent String enthalte auch keinerlei Informationen darüber, welche Apps oder Websites ein Nutzer besucht habe. Deshalb ermögliche er entgegen der Behauptung des Klägers auch keinen Überblick über das Internetnutzungsverhalten der Betroffenen und keine sehr intimen Einsichten. In Wahrheit enthalte der Consent String lediglich die Informationen, die erforderlich seien, um entsprechend den gesetzlichen Anforderungen die Erteilung und den Inhalt der vom Nutzer gegebenen Einwilligung feststellen und nachweisen zu können. Es sei auch klarzustellen, dass ein TC String erst dann im Speicher des Nutzerrechners abgelegt werde, wenn der Nutzer mit der CMP interagiere, also eine der Schaltflächen betätigt habe.

46
Es treffe schließlich nicht zu, dass „die streitgegenständlichen Datenübermittlungen“ auch erfolgten, wenn der Nutzer nicht mit der CMP interagiere und/oder keine bestätigende Handlung vorgenommen habe. Wichtig sei, dass an jede Domäne nur die Daten herausgegeben würden, deren Ablage in diesen

Speicherbereichen sie ausgelöst habe. Es sei daher falsch, wenn der Kläger den Eindruck erwecke, es werde hier gewissermaßen das Scheunentor geöffnet, durch das Außenstehende plötzlich alle denkbaren Daten aus dem Browser des Nutzers abziehen könnten. Vorsorglich sei darauf hinzuweisen, dass im Fall von Drittinhalten bzw. Drittanbietertechnologien der Informationsaustausch unmittelbar zwischen dem Nutzerrechner und dem Server des Dritten stattfinde und die Beklagte insoweit auch nicht an der Speicherung oder dem Auslesen von Informationen auf dem Endgerät des Nutzers teilnehme. Die Behauptung des Klägers, wonach die Beklagte aufgrund von Third-Party-Cookies Endgeräteinformationen im Webspeicher des Browsers von Nutzern speichere, sei daher unsinnig und falsch. Es werde zudem mit Nichtwissen bestritten, dass der Browser, mit dem die als Anlagen K 63 bis K 65 vorgelegten Bildschirmdarstellungen erzeugt worden sei, zuvor bereinigt worden sei, indem vor Aufruf der Website der Beklagten alle Cookies und Website-Daten entfernt worden seien, die den Cache des Browsers belegen würden. Diese Aussage zeuge bereits vom technischen Unverständnis des Klägers. Denn Cookies, der Browserverlauf oder auch der Downloadverlauf würden nicht im sog. Cache des Browsers (also dem Zwischenspeicher) gespeichert. Der Cache spielt hier keine Rolle. Die Beklagte gehe davon aus, dass der auf den Screenshots angezeigte Speicher vor Aufruf der Website www.focus.de nicht (ordnungsgemäß) bereinigt bzw. geleert worden sei. Ein Bildschirmfoto des bereinigten Speichers werde nicht vorgelegt. Schon deshalb hätten die Ausdrucke keinerlei Beweiswert bezüglich des Inhalts des Web-Speichers. Richtigkeit und Aussagekraft der vorgelegten Bildschirmausdrucke würden vor dem Hintergrund der zahlreichen Interaktionen des Klägers mit www.focus.de bestritten. Es sei der Beklagten auch nicht möglich, nachträglich diese Rahmenbedingungen nachzustellen. Daher bestreite sie vorsorglich mit Nichtwissen, dass ein neu aufgesetzter Browser nach dem Besuch der Seite www.focus.de zu dem vom Kläger angegebenen Zeitpunkt den Web-Speicher-Inhalt gehabt hätte, den die von ihm vorgelegten Screenshots zeigten. Falsch sei auch die Behauptung des Klägers, durch die Beklagte werde bei First Party-Cookies domainübergreifend das Nutzerverhalten nachvollzogen und ausgewertet. Drittanbieter könnten bei First Party-Cookies nicht - wie der Kläger meine - auf Informationen aus Endgeräten von Nutzern zugreifen. An dem Beispiel der vom Kläger bemängelten First Party-Cookies mit den Bezeichnungen „_ga“ und „_gid“ könne man der Anlage K 66 entnehmen, dass den Cookies „_ga_CV“ und „_ga“ nur eine Lebensdauer von max. 30 Minuten und bei „_gid“ 24 Stunden zugemessen seien. Derart kurzlebige First Party-Cookies seien von vornherein ungeeignet, um die vom Kläger als Gefahr ausgemalte „Nachverfolgung über einen ausgedehnten Zeitraum und mehrere Domänen hinweg“ zu ermöglichen. Diese Cookies unterfielen auch bereits nicht dem Klageantrag.

47
Im Übrigen nutze die Beklagte über einen sog. Reseller als technisch notwendigen Dienst das Tool „Google Analytics 360“ in einer modifizierten und eingeschränkten Version, wobei keine Daten mit Google geteilt und auch keine Daten in die USA übermittelt werden würden. Die Beklagte übermittele insbesondere keinerlei Cookie-Daten wie die Cookie-ID an Google. Die Beklagte habe Google Analytics bewusst so aufgesetzt. So seien in der Version von Google Analytics, die die Beklagte nutze, alle Google-Zusatzdienste wie AdSense, AdMob etc. deaktiviert. Ein Cookie werde hierbei lediglich als eine Art Session-Cookie für die Analyse des Nutzverhaltens auf der eigenen Webseite der Beklagten verwendet. Dieses Cookie werde 30 Minuten nach Ende der Session/des Webseitenbesuchs gelöscht. Der Webserver der Beklagten kommuniziere lediglich mit Google-Servern, um die Datei analytics.js von dort zu beziehen. Daneben nutze die Beklagte die Funktion Anonymize IP und könne daher keine Daten zusammenführen.

48
Entgegen den Ausführungen des Klägers diene auch das JavaScript „linkid.js“ in Google Analytics nicht zum domainübergreifenden Tracking. Tatsächlich sei „linkid.js“ lediglich ein sog. Plugin (Zusatzprogramm), das die sog. Enhanced Link Attribution (Optimierte Linkzuordnung) ermögliche. Enhanced Link Attribution verbessere die Genauigkeit der Nutzungsanalyse innerhalb einer Domäne durch die automatische Unterscheidung zwischen mehreren Links zur gleichen URL auf einer einzelnen Seite unter Verwendung von Linkelement-IDs. Hingegen ermögliche „linkid.js“ kein domänen- oder websiteübergreifendes Tracking.

49
Hinsichtlich der vom Kläger weiter erwähnten Speicherinhalte der „Local Storage“ und „Session Storage“ werde von dem Kläger nicht einmal behauptet, dass es einen Zusammenhang mit der „domainübergreifenden Aufzeichnung und Auswertung des Nutzerverhaltens zu Analyse- und Marketingzwecken“ gebe. Bei den vom Kläger vorgetragenen http-Anfragen an Domains von Drittparteien

gehe es noch nicht einmal um Cookies, sondern nur um den Aufruf etwa eines Dutzend Domains, von denen z.B. Inhalte über ein sog. Content Delivery Network bezogen würden (Cloudfront), die die IVW- und AGOF-Reichweitenmessung ermöglichten (INFOnline GmbH), die Wetterinformationen beisteuerten (The Weather Company) oder Ähnliches. Dies falle auch bereits nicht unter den Antrag, da es schon am Element der domainübergreifenden Aufzeichnung und Auswertung des Nutzerverhaltens fehle.

50
Soweit der Kläger behaupte, die Beklagte würde nach „vermeintlicher“ Zustimmung der Nutzer Third Party-Cookies von mindestens 18 fremden Domänen im Webspeicher der Browser von Nutzern „nebst User-ID“ speichern, sei dies falsch und werde bestritten. Eine Speicherung von „Third Party-Cookies“ erfolge nicht durch die Beklagte als Inhaberin der Domäne www.focus.de, sondern durch die jeweilige Drittpartei. Die „Third Party Cookies“ im Browser des Nutzers seien für die Beklagte genauso fremd wie für jeden Außenstehenden. Sie könne diese weder setzen noch auslesen. Schließlich werde aber auch schon die Behauptung (mit Nichtwissen) bestritten, dass von allen in der Liste auf der linken Seite der Anlage K 63 aufgeführten Domänen ein Cookie gesetzt worden sei.

51
Zudem sei klarzustellen, dass allein die Abspeicherung eines „Cookies“ nicht auf eine Aufzeichnung oder Auswertung des Nutzerverhaltens zu Analyse- oder Marketingzwecken schließen lasse.

52
Der Kläger konkretisiere bereits nicht, welche (angebliche) Verletzungshandlung der Beklagten er eigentlich angreifen möchte. Insbesondere fehle jegliche Darlegung einer Speicherung von Informationen auf dem Endgerät des Nutzers oder eines Zugriffs auf Informationen, die bereits im Endgerät des Nutzers hinterlegt seien, zum Zweck der domainübergreifenden Aufzeichnung und Auswertung des Nutzerverhaltens zu Analyse- und Marketingzwecken durch die Beklagte. Der Kläger trage lediglich zu angeblichen Informationsspeicherungen auf Nutzerrechnern durch die Beklagte vor und erkläre „websiteübergreifendes ‚Cross-Domain-Tracking‘“ zum Gegenstand seines Antrags, aber er zeige nicht auf, dass die Beklagte solches betreibe.

53
Soweit der Kläger behaupte, bei der Versteigerung von Werbeflächen würden zuvor gesammelte Profilinformationen faktisch mit versteigert, sei dies unzutreffend. Bei dem sogenannten „Cookie-Matching“ bringe der Ersteigerer selbst die Profilinformationen mit und die Werbetechnologie ermögliche es lediglich dem Ersteigerer, eine diesem Nutzer zuzuordnende Adimpression zu erwerben. Die vom Kläger geschilderten Abläufe zum System der Echtzeitversteigerung („Real Time Bidding“ oder „RTB“) seien fehlerhaft. Jedenfalls würden sich alle dort geschilderten Abläufe außerhalb des Verantwortungs- und Einflussbereichs der Beklagten abspielen.

54
Bezüglich des vom Kläger dargestellten Beispiels einer Echtzeitversteigerung auf der Webseite der Beklagten führt die Beklagte u.a. aus, dass die Formulierung des Klägers, es werde „mittels Cookies („Set-Cookie“) unter dem Namen „uuid2“ von Xandr Inc. auf Endgeräteinformationen zugegriffen“ insofern wenig Sinn ergebe, als Cookies hier als Instrument eines Endgerätezugriffs dargestellt würden, so als handele es sich bei ihnen um Software-Werkzeuge. In Wahrheit seien Cookies selbst die Information, die ggf. auf einem Endgerät gespeichert würden. Der allgemeinsprachlich verständliche Befehl „Set-Cookie“ (zu Deutsch: Setze Cookie) weise auch - entgegen der Darstellung des Klägers - gerade nicht auf einen Zugriff auf Endgeräteinformationen hin, sondern auf die Abspeicherung von Informationen auf dem Endgerät des Nutzers. Der Kläger erkläre auch in keiner Weise, welche Endgeräteinformationen angeblich an eine Vielzahl von Einkaufsplattformen „preisgegeben“ worden sein sollen. Der Kläger gebe auch nicht an, ob es sich um einen „bereinigten“ Browser gehandelt und/oder welche Cookie-Einstellungen er beim angeblichen Besuch der Website der Beklagten (oder zu einem früheren Zeitpunkt auf anderen besuchten Websites) vorgenommen habe.

55
Die Beklagte führt weiter aus, die Vorlage von Prüfprotokollen, in denen undifferenziert alle Cookies, Third Party Requests usw. aufgeführt würden, könne einen geordneten, auf den gestellten Antrag bezogenen Sachvortrag des Klägers nicht ersetzen. Es bleibe gänzlich im Unklaren, welche Prozesse nach Auffassung des Klägers unter den Klageantrag fielen. Die aufgeführten „First Party Cookies“ schieden bereits beim

Kriterium „domainübergreifend“ aus. Bei den „Third Party Cookies“ fehle es definitionsgemäß an einer Speicherung von Informationen auf dem Endgerät des Nutzers durch die Beklagte. Die Beklagte lese diese Cookies auch nicht aus, greife also nicht auf Informationen zu. Auch bei den aufgelisteten „Drittanfragen“ fehle es an Vortrag, dass Informationen auf dem Endgerät des Nutzers gespeichert bzw. dass auf solche bereits gespeicherten Informationen durch die Beklagte zugegriffen würde. Falsch sei auch, dass bei Besuch der Webseite www.focus.de von der Beklagten Anfragen an die Anbieter von Tracking-Diensten nebst IP-Adressen versendet würden. Diese Anfragen sende der Nutzerrechner direkt, ohne Einschaltung des Webservers der Beklagten, und auch eine etwaige Cookie-Setzung oder andere Informationshinterlegung auf dem Nutzerrechner nach der Verbindungsherstellung erfolge durch den Drittanbieter direkt, ohne Beteiligung der Beklagten.

56
Bezüglich der von dem Kläger behaupteten Vorgänge am 15.11.2021 bestreitet die Beklagte u.a. mit Nichtwissen, dass in der angeblichen Serveranfrage „Cookie-Informationen zum Abgleich mit Drittanbieter-Plattformen (Matching ID)“ und/oder „Parameter für die Auktion“ und/oder „Serverinformationen“ enthalten gewesen seien. Der Wert des Cookies „uuid2“ würde nach der allgemeinen Funktionsweise des HTTP-Protokolls mit einer Serveranfrage an den Server, der es zuvor gesetzt hat, zurückgegeben werden. Der Anlage K 81 sei allerdings nicht zu entnehmen, ob es eine solche vorangegangene Cookie-Setzung gegeben habe. „Angaben zu Browser-Einstellungen des Nutzers“ seien in gewissem Umfang Gegenstand jeder Kommunikation auf Basis des HTTP-Protokolls.

57
Die Beklagte habe auch nicht gezielt eine Funktion „Push Pages“ von Google implementiert. Die von dem Kläger angegebene URL https://pagead2.googlesyndication.com werde Seitenbetreibern von Google schon seit langer Zeit zur Einbindung der sog. Adsense-Werbung vorgegeben. Diese URL habe - nach Kenntnis der Beklagten - mit der Funktion „Push Pages“ von Google nichts zu tun. Die weiteren Schilderungen zu „Google Push Pages“ bestreitet die Beklagte: Hinter dieser Technik stehe das sog. „Cookie Matching“, das einem potenziellen Käufer von Werberaum ermögliche, die Informationen, die er bereits über einen Nutzer (Client) besitze, auch für Transaktionen über die Werbetechnologie von Google zu verwenden (vgl. Beschreibung seitens Google, Anlage B 3). Der Parameter „google_push“ könne nicht zur Identifikation verwendet werden, weil er unter anderem einen Zeitstempel enthalte und daher jedes Mal anders laute, wenn ein Nutzer eine Webseite besuche. Jeder Parameter sei einzigartig. Hierdurch habe Google die Möglichkeit ausgeschlossen, dass „google_push“ dazu verwendet werde, Daten von mehreren Käufern zusammenzuführen.

58
Die Beklagte wende auch kein Browser-Fingerprinting an, d.h. die Beklagte speichere keine „endgerätebezogenen Browserinformationen“ zur Erfassung des Nutzerverhaltens.

59
Bei AMP (Accelerated Mobile Pages, wörtlich übersetzt beschleunigte Mobilseiten) handele es sich um ein speziell für die Erstellung von Websites für mobile Endgeräte (v. a. Smartphones) entwickeltes Derivat von HTML (vgl. Anlage B 24). Auch die AMP-Seite unter amp.focus.de liege auf der Domain der Beklagten, nicht auf der Domain eines Dritten. Das Content Delivery Network „AMP Cache“ nutze die Beklagte nicht. Entgegen der Auffassung des Klägers sage das Format einer Seite (AMP oder non-AMP) nichts darüber aus, unter welcher Domain die Seite abrufbar sei.

60
Die Beklagte ist der Auffassung,

die vom Kläger vorgenommene Klageänderung sei unzulässig. Der Kläger stütze seinen Antrag nunmehr auf einen völlig neuen Klagegrund. Die fehlende Sachdienlichkeit der Klageänderung ergebe sich vorliegend insbesondere aus dem Umstand, dass durch die geänderte Klage im Ergebnis die „alte Sachlage“ anhand der „neuen Rechtslage“ erstrebt werden würde. Denn der bis zur Klageänderung von dem Kläger vorgebrachte Tatsachenstoff beziehe sich auf den Zeitraum vor der Entscheidung des BGH „Cookie-Einwilligung II“. Hieran sei aus prozessökonomischen Gründen kein legitimes Interesse anzuerkennen. Die Beklagte habe sich nunmehr auf die Änderungen der Sachlage eingestellt und verwende keines der früher üblichen „Cookie-Banner“ mehr.

61
Die Beklagte meint, der Kläger sei auch nicht aktivlegitimiert. Da er im vorliegenden Verfahren keine Verletzung datenschutzrechtlicher Vorschriften rüge, könne er seine Klagebefugnis auf § 2 Abs. 2 S. 1 Nr. 11 UKlaG stützen. Aus den ePrivacyrechtlichen Bestimmungen (§ 15 Abs. 3 TMG in richtlinienkonformer Auslegung, § 25 TTDSG) lasse sich nicht ableiten, dass bei jeder Cookie-Setzung alle Informationspflichten der DSGVO (Art. 13, Art. 26 Abs. 2 Satz 2) erfüllt sein müssten. Es müssten lediglich die Informationen gegeben werden, die für eine informierte Einwilligung erforderlich seien. Der Kläger könne seine Klagebefugnis auch nicht auf § 25 TTDSG i.V.m. §§ 3 a, 8 Abs. 1, Abs. 3 UWG stützen. § 25 TTDSG sei nicht als Marktverhaltensvorschrift einzuordnen. Eine Klagebefugnis lasse sich auch nicht aus § 5 Abs. 1 Satz 2 Nr. 7 UWG i.V.m. §§ 3, 8 Abs. 1, Abs. 3 UWG ableiten. Zunächst überzeuge bereits die Auffassung nicht, in jeder (vermeintlich) unzureichenden Einwilligungseinholung sei zugleich eine zur Täuschung geeignete Angabe i.S.d. § 5 Abs. 1 Nr. 7 UWG zu sehen. Dies könne jedoch dahinstehen, da bereits keiner der gestellten Anträge sich auf die Art und Weise der Einwilligungseinholung beziehe.

62
Die Klage erweise sich auch nach der Klageänderung aufgrund unbestimmter Klageanträge als unzulässig. Abstrakt-generelle Regelungen könnten nicht Grundlage eines gerichtlichen Verbots sein. Der Antrag sei auch deswegen zu weitgehend, da es nicht zwingend sei, dass bei einem domainübergreifenden Vorgehen ein Dritter beteiligt sei. Dies lasse unberücksichtigt, dass die Beklagte eine Mehrzahl von Informationsangeboten unter verschiedenen Domains betreibe. Der Antrag zu 1) lasse bereits nicht erkennen, aufgrund welcher technischen Vorgänge der Kläger die Tatbestandsvoraussetzungen der streitgegenständlichen Norm als erfüllt ansehe. Der Kläger wiederhole weitestgehend den Gesetzeswortlaut. Der Kläger habe sich auch nicht auf eine konkrete Verletzungsform bezogen, sondern lediglich auf eine sehr abstrakte Zweckbeschreibung. Auch die Angabe „zu Analyse- und Marketingzwecken“ sei unscharf.

63
Die Beklagte meint, die Klage sei im Übrigen auch nicht begründet. Es liege ein Fehlverständnis des Rechtsinstituts der sekundären Darlegungslast zugrunde, wenn der Kläger meine, er könne die von ihm beklagten Schwierigkeiten bei der Ermittlung des Sachverhalts, auf den er seine Ansprüche stützen möchte, auf die Beklagte abwälzen. Das Problem des Klägers liege in Wahrheit auch nicht darin, dass er keinen Einblick habe, was bei Besuch der Website der Beklagten passiere, sondern in seiner Weigerung, den Gegenstand seines Antrags zu konkretisieren. Allein schon deshalb sei es aber der Beklagten keinesfalls zumutbar, seine pauschalen Vorwürfe und Behauptungen durch detaillierte Darlegungen zu beantworten. Es sei für den Kläger auch kein Problem, die Cookie-Setzungen, die bei Besuch der Website der Beklagten zu einem bestimmten Zeitpunkt erfolgten, zu ermitteln und zu benennen. Es sei der Beklagten überdies technisch gar nicht möglich, abstrakt mitzuteilen, welche Cookies auf ihren Seiten zu welchen Zeitpunkten und zu welchen Zwecken tatsächlich gesetzt werden würden. Denn dies hänge von mehreren Faktoren ab, die weder vorhersehbar noch reproduzierbar seien. Die vom BGH für die sekundäre Darlegungslast aufgestellte Voraussetzung, dass „der Bestreitende alle wesentlichen Tatsachen kennt und es ihm unschwer möglich und zumutbar ist, nähere Angaben zu machen“, sei im Ergebnis nicht erfüllt. Der Nutzer einer Website könne Cookie-Setzungen feststellen - der Seitenbetreiber könne dies hingegen bei Third Party-Cookies nicht. Im Übrigen fehle es an dieser Zumutbarkeit auch deshalb, weil die Beklagte bei den „von den Drittanbietern bereitgestellten Tracking-Technologien“ gar nicht diejenige sei, die Informationen „auf dem Endgerät des Nutzers speichere oder auf Informationen zugreife, die bereits im Endgerät des Nutzers hinterlegt seien“.

64
Die Beklagte ist ferner der Auffassung, es sei falsch, dass die Beklagte Tracking-Technologien „unstreitig“ nutze, ohne dafür eine entsprechende Einwilligung einzuholen. Soweit eine Einwilligung erforderlich sei, werde diese auf der Seite der Beklagten auch wirksam eingeholt. Die Einwilligung erfolge freiwillig. Die Nutzer hätten die uneingeschränkte Möglichkeit, ihre Einwilligung zu verweigern. Die Einwilligung erfolge auch für den bestimmten Fall. So könnten Nutzer auch einfach alle Sponsoren ablehnen. Die Beklagte gebe ihren Nutzern sowohl die ausführliche Auswahlmöglichkeit als auch die einfache Zustimmungs- oder Ablehnungsmöglichkeit. Aus den gleichen Gründen liege auch eine „unmissverständlich abgegebene Willenserklärung“ vor. Die Wirksamkeit der Einwilligung werde auch nicht durch eine vermeintliche Irreführung der Nutzer in Frage gestellt. Der Kläger könne seine Argumente nicht aus der DSGVO ableiten,

wenn er sich auf diese nicht mehr stütze. § 25 TTDSG statuiere keine eigenständigen Informationspflichten. § 25 Abs. 1 S. 2 TTDSG beziehe sich nur auf die Fälle des voranstehenden Satzes 1, also die Fälle in denen eine Einwilligung erforderlich sei. Bei den „unbedingt erforderlichen Cookies“ i.S.d. § 25 Abs. 2 Nr. 2 TTDSG bestünden dagegen keinerlei Informationspflichten. Die Übermittlung der für jede Kontaktaufnahme im Internet technisch notwendige Informationen stelle keinen Informationszugriff dar (unter Hinweis auf die „Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 01. Dezember 2021, OH Telemedien 2021, vom 20.12.2021, Anlage B 23). In Bezug auf die IP-Adresse und die Browserinformationen fehle es an einem Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert seien.

65
Die Ausführungen des Klägers zum Verfahren der belgischen Aufsichtsbehörde (APD) über das IAB Europe und das TCF seien nicht entscheidungserheblich für das vorliegende Verfahren. Dieses Verfahren habe für den vorliegenden Rechtsstreit schon aufgrund seines Gegenstands keine Relevanz. Es befasse sich nur mit datenschutzrechtlichen Fragen und insoweit auch spezifisch mit der Verantwortlichkeit des IAB Europe als Initiator des TCF. Das Verfahren beziehe sich auch nur auf einen kleinen Ausschnitt aus den technischen Vorgängen, die vom Klageantrag des vorliegenden Verfahrens erfasst sein würden. Selbst wenn feststünde, dass das IAB Europe gegen Datenschutzbestimmungen verstoßen habe, ließe sich daraus nicht ableiten, dass die hiesige Beklagte unzulässige Informationsspeicherungen/-abrufe auf/aus Nutzerrechnern vorgenommen habe. Zwischen den in den beiden Verfahren entscheidungserheblichen Fragen bestehe auch keine Deckungsgleichheit. Insbesondere lasse sich der APD-Entscheidung nicht entnehmen, wie die große Bandbreite der vom Klageantrag erfassten Informationsspeicherungen/-abrufe unter dem Blickwinkel der ePrivacy-Richtlinie zu bewerten sei und ob die mittels der CMP der Beklagten eingeholten Einwilligungen wirksam seien. Im Übrigen sei die Entscheidung nicht rechtskräftig. Die Informationsverarbeitung in dem Consent String sei jedenfalls zwingend zur Einwilligungsverwaltung erforderlich ist und daher jedenfalls - soweit überhaupt eine Verarbeitung personenbezogener Daten bzw. eine Informationsspeicherung in/Informationsauslesung aus dem Nutzerendgerät vorliege - gem. Art. 6 Abs. 1 Buchst. f) bzw. § 25 Abs. 2 Nr. 2 TTDSG als zulässig anzusehen.

66
Wegen der weiteren Einzelheiten des Parteivorbringens wird auf die wechselseitigen Schriftsätze samt Anlagen sowie die Sitzungsniederschriften vom 23.11.2021 (Bl. 501/503 d.A.) und 12.07.2022 (Bl. 661/633 d.A.) Bezug genommen.

67
Mit Beschluss vom 23.11.2021 wurde das Passivrubrum von Focus Online Group GmbH hin zu BurdaForward GmbH berichtigt (Bl. 501/503 d.A.). Aufgrund Beschlusses vom 12.07.2022 (Bl. 631/633 d.A.) wurden die Akten dem zuständigen Bayerischen Landesamt für Datenschutzaufsicht (BayLDA) zum Zwecke der Anhörung gem. § 12 a UKlaG zugeleitet. Dieses hat mit Schreiben vom 09.09.2022 Stellung genommen (Bl. 646/663 d.A.). Hierauf gingen nicht nachgelassene Schriftsätze der Beklagten vom 30.09.2022 (Bl. 665/666), vom 10.11.2022 (Bl. 672/693 d.A.) und vom 21.11.2022 (Bl. 694/698 d.A.) sowie des Klägers vom 06.10.2022 (Bl. 667/668 d.A.) ein.

## Entscheidungsgründe

68
Die zulässige Klage ist nur bezüglich des Klageantrags Nr. 1 begründet. Im Übrigen ist sie unbegründet.

69
A. Die Klage ist zulässig, insbesondere sind die Klageanträge in der zuletzt gestellten Form ausreichend bestimmt.

70
I. Es bestehen keine Bedenken im Hinblick auf die Zulässigkeit der Auswechslung der Klageanträge, wie sie der Kläger mit Schriftsätzen vom 25.09.2020 (Bl. 253/264 d.A.) und vom 11.01.2021 (Bl. 298/366 d.A.) jeweils vorgenommen hat. Soweit der Kläger seine Anträge zuletzt nur noch auf das TTDSG stützt, handelt es sich um eine Klageänderung, die sachdienlich ist, § 263 ZPO:

71

1. Der Streitgegenstand wird nach der Rechtsprechung durch den Klageantrag, in dem sich die von dem Kläger in Anspruch genommene Rechtsfolge konkretisiert, und den Lebenssachverhalt (Anspruchsgrund) bestimmt, aus dem der Kläger die begehrte Rechtsfolge ableitet. Eine Klageänderung liegt vor, wenn entweder der Klageantrag oder der Klagegrund ausgewechselt wird (BGH NJW 2008, 3570 m. w. Nachw.). Die Identität des Klagegrundes wird aufgehoben, wenn durch neue Tatsachen der Kern des in der Klage angeführten Lebenssachverhalts verändert wird. Dabei muss es sich um wesentliche Abweichungen handeln; die bloße Ergänzung oder Berichtigung der tatsächlichen Angaben fällt unter § 264 Nr. 1 ZPO und stellt daher keine Änderung des Klagegrundes dar (NJW 2007, 83 Rn. 11 - Lesezirkel II).

72
Vorliegend hat der Kläger die ursprünglich mit der Klageschrift angekündigten Anträge auf Verstöße gegen die DSGVO gestützt, wie aus dem Wortlaut der Klageanträge sowie aus deren Begründung im Einzelnen hervorgeht. Insbesondere richtete sich der Kläger dabei ursprünglich gegen die Verarbeitung von personenbezogenen Daten im Sinne von Art. 4 Nr. 1 DSGVO. Der Kläger hat dies mit Schriftsatz vom 25.09.2020 nochmals bestätigt, indem er darauf hinwies, dass im Zeitpunkt der Klageerhebung mangels Umsetzung der ePrivacy-Richtlinie ausschließlich die DSGVO auf die angegriffenen Technologien für anwendbar erachtet worden sei (vgl. Bl. 253 ff. d.A.). Indem der Kläger seine Anträge zuletzt auf einen Verstoß gegen das TTDSG beschränkt hat, hat er den Klagegrund ausgewechselt. Eine weitere Änderung des Klagegrunds liegt in der Auswechslung des angegriffenen Einwilligungsmechanismus, den die Beklagte erst nach Klageerhebung nutzte (sogenannte CMP, vgl. Schriftsatz vom 11.01.2021, Bl. 298/366 d.A.). Dabei handelt es sich weder um eine Ergänzung oder Berichtigung des bisherigen Vortrags, sondern um eine wesentliche neue Tatsache, die den bis dahin zugrunde gelegten Lebenssachverhalt erheblich verändert hat. Schließlich hat der Kläger auch den Klageantrag in wesentlichen Punkten geändert, in dem er nicht mehr allein auf die Verarbeitung personenbezogener Daten abgestellt und auch in seinen Klageanträgen ausdrücklich auf die neue Form des angegriffenen Einwilligungsmechanismus Bezug genommen hat (vgl. den ausdrücklichen Verweis in den Anträgen auf die Anlagen K 58, K76 und K 80).

73
2. Es handelt sich dabei jeweils um eine zulässige Klageänderung, die unter prozessökonomischen Gesichtspunkten sachdienlich ist, da zwischen den angegriffenen Verhaltensweisen jedenfalls ein sachlicher Zusammenhang besteht:

74
Für die Beurteilung der Sachdienlichkeit kommt es nach der Rechtsprechung allein auf die objektive Beurteilung an, ob und inwieweit nämlich die Zulassung der Klageänderung der Ausräumung des sachlichen Streitstoffes im Rahmen des anhängigen Rechtsstreits dient und einem andernfalls zu gewärtigenden weiteren Rechtsstreit vorbeugt. Dabei ist es ohne Belang, ob die Zulassung der Klageänderung weitere Erklärungen der Parteien und neue Beweiserhebungen notwendig macht, da nicht die beschleunigte Erledigung dieses Prozesses, sondern die Erledigung der Streitpunkte zwischen den Parteien für die Frage der Sachdienlichkeit maßgeblich ist. Es kann mit anderen Worten vom Standpunkt der Prozesswirtschaftlichkeit nicht als sachdienlich angesehen werden, wenn durch die Zurückweisung einer Klageänderung der Kläger geradezu zur Erhebung einer neuen Klage herausgefordert wird (BGH NJW 1951, 311).

75
Vorliegend geht es sowohl vor als auch nach Klageänderung im Kern um die Zulässigkeit der von der Beklagten eingesetzten Technologie, wobei auch zu berücksichtigen ist, dass auch das nunmehr gegenständliche TTDSG erhebliche Bezüge zur DSGVO aufweist. Insofern ist der Streitstoff im Kern trotz geänderten Klagegrunds und Klageantrags wesensgleich. Daran ändert auch die im Laufe des Prozesses durch die Entscheidung des BGH vom 28.05.2020 - Cookie-Einwilligung II, bzw. infolge des Inkrafttretens des TTDSG eintretende Änderung der Rechtslage nichts. Soweit die Beklagte der Auffassung ist, es bestünde aus prozessökonomischer Sicht kein Interesse daran, die alte Sachlage anhand der neuen Rechtslage zu beurteilen, ist dies angesichts der Klageänderung auch im Hinblick auf den neuen Einwilligungsmechanismus CMP unbehelflich. Denn durch die diesbezügliche Klageänderung kann vorliegend gerade die Erhebung einer neuen Klage verhindert werden. Auch der Auffassung der Beklagten, wonach die infolge der Klageänderungen eintretende Anwachsung des Klägervortrags einer Sachdienlichkeit entgegenstünde, kann nicht gefolgt werden. Denn zum einen kann den rechtlichen wie tatsächlichen Ausführungen des Klägers, auch soweit diese noch zur DSGVO ergangen sind, schon allein

aufgrund der gesetzlichen Verknüpfung zwischen § 25 Abs. 1 S. 2 TTDSG und der DSGVO nicht jegliche Relevanz abgesprochen werden; zum anderen gehört es zu den üblichen Vorgängen des Zivilprozesses, dass Sach- und Rechtsvortrag sich im Laufe des Prozesses ändern und zu einer Erhöhung des Umfangs und der Komplexität des Streitstoffs führen können.

76
Da die Klageänderung noch vor mündlicher Verhandlung erfolgt ist, kommt es auf die streitige Frage, ob bei einer Aufgabe des bisherigen Rechtsschutzbegehrens § 269 ZPO neben § 263 ZPO anwendbar ist (vgl. Greger in: Zöller, ZPO, 34. Auflage 2022, § 263 Rn. 6), im Ergebnis nicht an, da eine Einwilligung der Beklagten auch nach § 269 Abs. 1 ZPO nicht erforderlich war.

77
II. Die Anträge sind in der zuletzt gestellten Form auch hinreichend bestimmt, § 253 Abs. 2 Nr. 2 ZPO. Ein Unterlassungsantrag - und nach § 313 Abs. 1 Nr. 4 ZPO eine darauf beruhende Verurteilung - darf nicht derart undeutlich gefasst sein, dass der Streitgegenstand und der Umfang der Prüfungs- und Entscheidungsbefugnis des Gerichts (§ 308 I ZPO) nicht erkennbar abgegrenzt sind, sich der Beklagte deshalb nicht erschöpfend verteidigen kann und die Entscheidung darüber, was dem Beklagten verboten ist, letztlich dem Vollstreckungsgericht überlassen bleibt. Eine auslegungsbedürftige Antragsformulierung kann aber dann hinzunehmen sein, wenn eine weitergehende Konkretisierung nicht möglich und die gewählte Antragsformulierung zur Gewährung effektiven Rechtsschutzes erforderlich ist (BGH GRUR 2017, 422 - ARD-Buffet, m.w.Nachw.). Ein auf die Wiederholung des gesetzlichen Verbotstatbestands beschränkter Klageantrag genügt den Anforderungen an die Bestimmtheit grundsätzlich nicht (BGH GRUR 2010, 749 Rn. 21 - Erinnerungswerbung im Internet). Es ist aber nicht grundsätzlich unzulässig, in einem Klageantrag auslegungsbedürftige Begriffe zu verwenden. Die Anforderungen an die Konkretisierung des Streitgegenstands in einem Unterlassungsantrag sind dabei auch abhängig von den Besonderheiten des jeweiligen Sachgebiets (vgl. BGH GRUR 2002, 1088, 1089 - Zugabenbündel).

78
Nach diesen Grundsätzen sind die Klageanträge hinreichend bestimmt: Zwar benennt insbesondere der Klageantrag Nr. 1 nicht eine oder mehrere konkrete Technologien, die angegriffen werden sollen. Gleichwohl wiederholt der Antrag auch nicht lediglich den Wortlaut der insoweit streitentscheidenden Verbotsnorm des § 25 TTDSG, sondern betrifft nur einen Ausschnitt aus deren Anwendungsbereich, indem er Merkmale der angegriffenen Verletzungshandlungen benennt. Soweit der Klageantrag solche Zugriffe ausklammert, die unbedingt notwendig sind, bzw. für die „eine informierte und freiwillige Einwilligung der Nutzer“ eingeholt wird, handelt es sich zwar im Wesentlichen um eine Wiederholung des Gesetzeswortlauts (vgl. § 25 Abs. 1 S. 1 und Abs. 2 Nr. 2 TTDSG). Die Wiederholung solcher negativer Tatbestandsvoraussetzungen im Klageantrag erscheint jedoch unschädlich, solange aus dem Antrag im Übrigen eine ausreichende Konkretisierung folgt. Dies ist vorliegend der Fall: Denn der Klageantrag besteht nicht allein in der (abstrakt gehaltenen) Beschreibung der Verletzungshandlung, sondern aus zwei Teilen, die in einem wechselseitigen Verhältnis zueinander stehen und in einer Gesamtschau den Streitstoff abgrenzen. Zum einen wird das verbotene Verhalten durch Beschreibung der streitgegenständlichen Handlung, nämlich die Speicherung von bzw. der Zugriff auf Informationen auf dem Endgerät des Nutzers für die domainübergreifende Aufzeichnung und Auswertung des Nutzerverhaltens zu Analyse- und Marketingzwecken ausreichend erkennbar, zum anderen wird die beanstandete Einwilligungseinholung durch Bezugnahme auf die konkret beanstandete Form, namentlich die Anlage 58 (das konkret verwendete „Consent-Management-Tool“) genau bestimmt. Gerade diese Zweiteilung des Antrags macht es für die Beklagte hinreichend erkennbar, welche Verhaltensweisen durch den Antrag verboten werden sollen. Im Ergebnis wird der abstrakt formulierte Teil des Klageantrags durch die Bezugnahme auf den konkret angegriffenen Einwilligungsmechanismus hinreichend präzisiert, so dass die Beklagte nach Auffassung der Kammer erkennen kann, welche Verhaltensweisen vom Antrag umfasst sein sollen. Denn schließlich ist es die Beklagte, die mittels der angegriffenen CMP die Einwilligung der Nutzer zu konkret von ihr beschriebenen Diensten und Technologien einholt, welche im Übrigen - nach eigenem Vortrag der Beklagten - in deren Einwilligungsmechanismus auch hinreichend und transparent beschrieben werden. In dieser Hinsicht können im Übrigen auch die Klagebegründung sowie dazu gegebene Erläuterungen zur Bestimmung der Reichweite des Verbots heranzogen werden (vgl. Köhler/Bornkamm/Feddersen/Köhler/Feddersen, 40. Aufl. 2022, UWG § 12 Rn. 1.37 m.w.Nachw.).

79

Schließlich ist auch zu berücksichtigen, dass angesichts der Vielzahl an möglichen Technologien und den unterschiedlichen - je nach Anbieter wechselnden - Bezeichnungen von einer konkreten Benennung einer oder mehrerer Technologien auch kein maßgeblicher Mehrwert ausginge. Der von dem Kläger im dem ersten Teil abstrakt formulierte Antrag war daher auch vor dem Hintergrund des Gebots des effektiven Rechtsschutzes erforderlich. Würde man dagegen die Beschränkung des Klageantrags auf eine konkret benannte Technologie oder ein konkret zu benennendes Cookie verlangen, würde dies angesichts der Auswechselbarkeit der unterschiedlichen Formen des Trackings die Wirksamkeit eines Verbots entscheidend beinträchtigen. Es ist deshalb vorliegend hinzunehmen, dass bei der Beurteilung behaupteter Verstöße im Vollstreckungsverfahren auch Wertungen vorzunehmen sein werden. Hierdurch wird auch aus den oben genannten Gründen die Rechtsverteidigung der Beklagten und ihr schützenswertes Interesse an Rechtsklarheit und Rechtssicherheit hinsichtlich der Entscheidungswirkungen nicht unzumutbar beeinträchtigt. (BGH GRUR 2004, 696 - Abwerbeanruf durch Personalberater).

80
Soweit die Beklagte auch Bedenken gegen die Klageanträge Nr. 2 und 3 geltend macht, gelten die obigen Ausführungen entsprechend.

81
B. Die Klage ist nur in dem tenorierten Umfang begründet.

82
I. Der Kläger kann von der Beklagten gem. § 2 Abs. 1 S. 1, Abs. 2 S. 1 Nr. 11 UKlaG i.V.m. § 25 TTDSG verlangen, dass diese es unterlässt, für die domainübergreifende Aufzeichnung und Auswertung des Nutzerverhaltens zu Analyse- und Marketingzwecken Informationen auf dem Endgerät des Nutzers zu speichern oder auf Informationen zuzugreifen, wenn sie hierzu lediglich eine Einwilligung mittels des angegriffenen Einwilligungsmechanismus (TFC 2.0, vgl. Anlage K 58) einholt.

83
1. Entgegen der Auffassung der Beklagten folgt die Aktivlegitimation des Klägers, als in die Liste der qualifizierten Einrichtungen gemäß § 4 UKlaG aufgenommener Verbraucherschutzverein, aus § 2 Abs. 2 S. 1 Nr. 11 UKlaG i. V. m. § 25 TTDSG.

84
Nach § 2 Abs. 2 S. 1 Nr. 11 UKlaG gehören zu den Verbraucherschutzgesetzen i.S.d. § 2 auch die Vorschriften, die die Zulässigkeit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten von Verbrauchern („Verbraucherdaten“) regeln, wenn diese Handlungen zu kommerziellen Zwecken vorgenommen werden. Erfasst werden grundsätzlich alle innerstaatlich geltenden datenschutzrechtlichen Vorschriften (Köhler/Bomkamm/Feddersen/Köhler, 40. Aufl. 2022, UKlaG § 2 Rn. 17). Ob auch das am 01.12.2021 in Kraft getretene und der Umsetzung der Richtlinie 2002/58/EG (ePrivacy-RL) des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.07.2002, S. 37) dienende TTDSG hierunter fällt, ist - soweit ersichtlich - bislang nicht geklärt. Im Ergebnis ist dies zu bejahen:

85
a) Zu den ab dem 25.05.2018 geltenden Regelungen der DSGVO wurde etwa die Auffassung vertreten, dass § 2 Abs. 2 S. 1 Nr. 11 keine Grundlage in der DSGVO hätte und wegen des Vorrangs des Unionsrechts vor dem nationalen Recht jedenfalls ab dem 25.05.2018 nicht mehr angewendet werden dürfte. Die DSGVO solle auch nicht die kollektiven Interessen der Verbraucher, sondern die Grundrechte und Grundfreiheiten der Bürger schützen (Köhler/Bornkamm/Feddersen/Köhler, 40. Aufl. 2022, UKlaG § 2 Rn. 29g., zum Meinungsstand m.w.Nachw.: BGH GRUR 2020, 896 - App-Zentrum).

86
Die gleiche Argumentation - würde man dieser folgen - spräche auch gegen eine Anwendung des § 2 Abs. 2 S. 1 Nr. 11 UKlaG auf das TTDSG. Denn auch § 25 TTDSG geht auf eine unionsrechtliche Regelung, nämlich Art. 5 Abs. 3 ePrivacy-RL zurück, und setzt diese um.

87
Auf Vorlage des BGH (BGH GRUR 2020, 896 - App-Zentrum) entschied der EuGH jedoch den Streit in Bezug auf Verbraucherschutzverbände dahingehend, dass Art. 80 Abs. 2 der VO (EU) 2016/679 des

Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG (Datenschutz-Grundverordnung) dahin auszulegen sei, „dass er einer nationalen Regelung, nach der ein Verband zur Wahrung von Verbraucherinteressen gegen den mutmaßlichen Verletzer des Schutzes personenbezogener Daten ohne entsprechenden Auftrag und unabhängig von der Verletzung konkreter Rechte betroffener Personen Klage mit der Begründung erheben kann, dass gegen das Verbot der Vornahme unlauterer Geschäftspraktiken, ein Verbraucherschutzgesetz oder das Verbot der Verwendung unwirksamer Allgemeiner Geschäftsbedingungen verstoßen worden sei, nicht entgegensteht, sofern die betreffende Datenverarbeitung die Rechte identifizierter oder identifizierbarer natürlicher Personen aus dieser Verordnung beeinträchtigen kann.“ (EuGH GRUR-RS 2022, 8637 Rn. 67 ff. - Meta Platforms Ireland/Bundesverband).

88
b) Gleichwohl die Entscheidung des EuGH nicht zum TTDSG ergangen ist, sprechen angesichts der damit jedenfalls unionsrechtlich ausgeräumten Bedenken erhebliche Gründe für eine Anwendbarkeit des § 2 Abs. 2 S. 1 Nr. 11 UKlaG auf das TTDSG:

89
i) Denn zum einen unterfällt das TTDSG als Datenschutzvorschrift (vgl. BGH, Urt. v. 27.01.2022 - III ZR 4/21 -, Rn. 37, juris) dem Anwendungsbereich des § 2 Abs. 2 S. 1 Nr. 11 UKlaG. Auch regelt das TTDSG den Schutz personenbezogener Daten. Zwar ist der Anwendungsbereich von § 25 TTDSG breiter als derjenige von Art. 6 Abs. 1 DS-GVO, denn die betroffenen Informationen müssen nicht zwingend personenbezogen sein; auch diese werden aber vom Anwendungsbereich des TTDSG umfasst (MAH GewRS, 6. Auflage 2022 § 27 Rechtsfragen der Telemedien Rn. 133). Daher kommen beide Regelwerke dann zur Anwendung, wenn einwilligungsbedürftige Technologien nach Art. 5 Abs. 3 ePrivacy-RL auch personenbezogene Daten verarbeiten (Taeger/Pohle ComputerR-HdB, 1. Abschnitt. Teil 3. 33.2 Projektspezifischer Datenschutz Rn. 108).

90
ii) Zum anderen enthält der Datenschutz - wie § 1 Abs. 3 S. 1 TTDSG bestätigt - eine verbraucherschützende Komponente, da es zumindest auch um die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten von natürlichen Personen in ihrer Eigenschaft als Verbraucher durch Unternehmen als Teil des Marktes geht (vgl. Köhler/Bornkamm/Feddersen/Köhler, 40. Aufl. 2022, UKlaG § 2 Rn. 17). So wurde auch für das TMG, welches in den hier maßgeblichen Bereichen durch das TTDSG ab 01.12.2021 ersetzt wurde, die Anwendbarkeit des § 2 Abs. 2 S. 1 Nr. 11 UKlaG bejaht (Köhler/Bomkamm/Feddersen/Köhler, 40. Aufl. 2022, UKlaG § 2 Rn. 17; MüKoZPO/Micklitz/Rott, 6. Aufl. 2022, UKlaG § 2 Rn. 31).

91
iii) Nachdem auch der Anwendungsvorrang des Unionsrechts einer Anwendung des § 2 Abs. 2 S. 1 Nr. 11 UKlaG nicht entgegensteht und die Vorschrift nach allgemeiner Auffassung eine „dynamische Verweisung“ darstellt, die auch künftige Vorschriften einbezieht (Köhler/Bornkamm/Feddersen/Köhler, a.a.O.), folgt die Kammer der Auffassung, wonach auch das TTDSG eine Klagebefugnis des Klägers nach § 2 Abs. 2 S. 1 UKlaG begründet.

92
iv) Dem steht auch nicht die mit Beschluss des BGH vom 10.11.2022 (Az. I ZR 186/17 - App-Zentrum) erfolgte erneute Vorlage an den EuGH entgegen. Zum einen betrifft die Vorlagefrage - wie ausgeführt - nicht die Klagebefugnis aufgrund des TTDSG, zum anderen hat die Vorlage folgerichtig die - hier nicht relevante - Frage zum Gegenstand, ob eine Rechtsverletzung „infolge einer Verarbeitung“ im Sinne des Art. 80 Abs. 2 DSGVO vorliegt, wenn die sich aus Art. 12 Abs. 1 Satz 1, Art. 13 Abs. 1 Buchst. c und e DSGVO ergebenden Informationspflichten verletzt worden sind. Im vorliegenden Verfahren streitgegenständlich ist nämlich die Speicherung bzw. der Zugriff auf Informationen auf dem Endgerät des Nutzers. Eine Verarbeitung von personenbezogenen Informationen setzt § 25 TTDSG im Gegensatz zur DSGVO (vgl. § 1 Abs. 1 DSGVO) nicht voraus. Eine Verletzung infolge einer Verarbeitung läge im Übrigen unproblematisch vor (vgl. Art. 4 Nr. 2 DSGVO).

93

Vor diesem Hintergrund kommt trotz des laufenden Vorabentscheidungsverfahrens eine Aussetzung des Verfahrens nach § 148 Abs. 1 ZPO nicht in Betracht.

94
v) Darauf, ob § 25 TTDSG daneben auch eine Marktverhaltensnorm nach § 3a UWG darstellt, kam es mithin nicht mehr an.

95
2. Die Beklagte ist als Betreiberin dar Webseite www.focus.de auch passivlegitimiert, da es sich bei einem Online-Nachrichtenportal um einen elektronischen Informations- und Kommunikationsdienst (vgl. die Legaldefinition in § 1 Abs. 1 TMG), mithin um Telemedien im Sinne des § 2 Abs. 2 Nr. 1 TTDSG handelt. Gem. § 1 Abs. 3 TTDSG unterliegen dem TTDSG ferner alle Unternehmen und Personen, die im Geltungsbereich des Gesetzes eine Niederlassung haben oder Dienstleistungen erbringen oder daran mitwirken. Auch dies trifft auf die Beklagte mit Sitz in München zu.

96
3. Die Beklagte verstößt vorliegend gegen § 25 TTDSG, indem sie veranlasst, dass Cookies, insbesondere in Form des TC Strings, auf dem Endgerät des Nutzers gespeichert und zum „Tracking“ des Nutzers genutzt werden (c), ohne eine wirksame Einwilligung der betroffenen Nutzer einzuholen (d und e).

97
a) Nach § 25 TTDSG ist jede Speicherung von Informationen in Endeinrichtungen des Endnutzers oder der Zugriff auf bereits darin gespeicherte Informationen nur mit einer Einwilligung zulässig, die auf Grundlage einer klaren und umfassenden Information erfolgt sein muss.

98
b) Der Begriff Endeinrichtung in § 25 TTDSG knüpft an die Verarbeitungssituation an. Es muss sich um Informationen aus dem Herrschaftsbereich des „Endnutzers“ handeln, d.h. einer natürlichen Person, die den Telemediendienst verwendet (MAH GewRS, § 27 Rn. 130).

99
Unstreitig werden im Speicher der Endgeräte der jeweiligen Nutzer der Webseite www.focus.de sogenannte Cookies abgespeichert, wobei eine Speicherung teils auch bereits vor Interaktion mit dem Consent-Management-Tool der Beklagten erfolgt. Cookies sind Textdateien, die der Anbieter einer Internetseite auf dem Computer des Benutzers speichert und beim erneuten Aufrufen der Webseite wieder abrufen kann, um die Navigation im Internet oder Transaktionen zu erleichtern oder Informationen über das Nutzerverhalten abzurufen (BGH NJW 2020, 2540 Rn. 49 - Cookie-Einwilligung II; BGH GRUR 2018, 96 Rn. 15 - Cookie-Einwilligung I; vgl. auch MAH GewRS Rn. 133).

100
c) Zwischen den Parteien ist allerding umstritten, in welcher Anzahl, zu welchem Zweck und zu welchem Zeitpunkt derartige Informationen abgespeichert werden. Unstreitig wird jedoch der sogenannte TC String, eine codierte Zeichenkette, nach Abfragen der Einwilligung durch die CMP auf dem Rechner des Nutzers als Cookie gespeichert.

101
i) Nach Vortrag der Beklagten soll der TC String die relevanten Informationen im Hinblick auf die Nutzereinwilligung, nicht dagegen Informationen darüber, welche Apps oder Websites ein Nutzer besucht habe, enthalten und auch keinen Überblick über das Intemetnutzungsverhalten der betroffenen Nutzer ermöglichen.

102
ii) Dem kann nicht gefolgt werden. Nach Überzeugung der Kammer handelt es sich zumindest bei dem von der Beklagten auf den Endgeräten der Nutzer als Cookie gespeicherten TC String um eine personenbezogene Information, die der domainübergreifenden Nachverfolgung der Nutzer dient, wobei dies auch zu Analyse- und Marketingzwecken erfolgt.

103
iii) Der TC String dient - wie die Beklagte selbst ausführt - im Rahmen des TCF-Netzwerks als Kommunikationsmittel für Abfrage und Übermittlung der Nutzereinwilligung zwischen Publishem, Werbungireibenden, Vermarktern, Agenturen und ihren jeweiligen Technologiepartnem. Bereits aus dieser

Zwecksetzung wird ersichtlich, dass die Einverständnis-/Ablehnungsauswahl des jeweiligen Nutzers einem Individuum zugeordnet werden soll. Denklogische Voraussetzung hierfür ist, dass der jeweilige Nutzer identifiziert werden kann. So enthält der TC String nach der von dem Kläger in Bezug genommenen Entscheidung der belgischen Datenschutzbehörde l'Autorité de protection des données (APD) u.a. (S. 64 f., Rn. 301) folgende Inhalte:

allgemeine Metadaten; Binärwert für jeden Verarbeitungszweck, für den eine Einwilligung gegeben werden kann; Binärwert für jeden Verarbeitungszweck, der mit berechtigtem Interesse erfolgt; Binärwert für jeden Adtech-Vendor, der auf Basis einer Einwilligung des Nutzers Daten sammeln und verarbeiten darf; Binärwert für jeden Adtech-Vendor, dessen Verarbeitung auf einem berechtigten Interesse beruht; jedwede Verarbeitungsbeschränkung; Einverständnis in solche Verarbeitungen, die nicht vom TCF gedeckt sind.

104
Zwar geht die belgische Datenschutzbehörde davon aus, dass aufgrund der oben festgestellten Inhalte nicht abschließend festgestellt werden kann, dass der TC String die direkte Identifikation des Nutzers ermögliche. Allerdings stellt die Behörde in ihrer Entscheidung fest, dass aufgrund der Anzeige des Zustimmungs-Popups, das durch einen von dem CMP verwalteten Server mittels Skripts abgerufen wird, zwangsläufig auch die IP-Adresse des Nutzers verarbeitet werde (vgl. a.a.O. S. 66, Rn. 319). Sei der TC String als Cookie einmal auf dem Endgerät gespeichert, ermögliche die CMP eine eindeutige Identifizierung in Form der Zuordnung einer IP-Adresse (a.a.O. S. 82, Rn. 375). Um dem Nutzer die CMP anzuzeigen, müsse der „Publisher" die CMP mittels eines Java Script-Codes auf seiner Webseite implementieren. Dieser Code werde dann direkt von dem CMP Server oder über eine Sub-Domain geladen. Infolge dieser HTTP(S)-Anfrage erhielten sowohl der Server des Publishers als auch der CMP-Server Zugriff zu der IP-Adresse des Nutzers, welcher die Webseite besuche und das CMP-Interface sehe. Dieser Zugriff ermögliche der CMP, die im TC String enthaltenen Informationen mit weiteren Informationen anzureichern, die sich bereits in ihrem Besitz oder im Besitz des Publishers befänden und mit derselben IP-Adresse verknüpft seien (a.a.O. S. 82, Rn. 376 f.). Die belgische Datenschutzbehörde geht daher davon aus, dass durch die CMP eine große Zahl an personenbezogenen Daten verarbeitet werden. Auch im Rahmen des Real-Time-Bidding-Prozesses enthalte die Gebotsanfrage den TC-String, der die Präferenzen des Webseiten-Besuchers angebe.

105
Die oben widergegebene Beurteilung des TFC 2.0 durch die belgische Datenschutzbehörde ist auch für den gegenständlichen Rechtsstreit relevant. Aus dem Umstand, dass die belgische Behörde die Zulässigkeit nach datenschutzrechtlichen Gesichtspunkten beurteilt, folgt bereits nicht, das die dort festgestellten technischen Vorgänge bei der Würdigung des streitgegenständlichen klägerischen Vortrags nicht zugrunde gelegt werden könnten. Im Übrigen überschneiden sich vorliegend der Anwendungsbereich der DSGVO und des TTDSG (siehe bereits oben unter I.1.b.i).

106
iv) Unter Berücksichtigung des klägerischen Vortrags, der Einlassungen des Beklagten hierzu sowie der oben angesprochenen Entscheidung der belgischen Datenschutzbehörde geht die Kammer davon aus, dass beim Aufruf der Webseite www.focus.de der TC String - jedenfalls nach Interaktion des Nutzers mit der CMP - in Form einer Textdatei (als Cookie) auf dem Endgerät des Nutzers abgespeichert und diese zugleich an die CMP übermittelt wird. Hierin enthalten sind danach Informationen wie Browser- und Geräteinformationen, die entsprechend getätigten Präferenzen sowie die IP-Adresse des Nutzers. Die Kammer folgt der belgischen Entscheidung auch dahingehend, dass es sich bei den geteilten Daten um personenbezogene Informationen handelt, ohne dass es hierauf entscheidend ankäme. Diese Informationen werden - jedenfalls nach einer entsprechenden Einwilligungserteilung des Nutzers - an Dritte, die sogenannten Vendoren, weitergeleitet, was eine domainübergreifende Aufzeichnung der persönlichen Daten und deren Auswertung, insbesondere im Rahmen des Real-Time-Biddings, miteinschließt. So führt die belgische Datenschutzbehörde in ihrer Entscheidung u.a. aus, dass, wenn ein Benutzer bewusst oder unbewusst seine Einwilligung über die Schaltfläche „Alles akzeptieren" erteilt habe und weder der Webseitenbetreiber noch die CMP von der vollständigen Liste der teilnehmenden adtech-Vendoren abgewichen seien, die persönlichen Daten der betroffenen Person mit hunderten von Dritten geteilt werden würden (a.a.O., S. 85, Rn. 393). Der Zweck einer solchen Datenübermittlung ergibt sich zur Überzeugung der Kammer bereits aus den Informationen, wie sie die Beklagte bei ihrer Einwilligungsabfrage selbst erteilt. So informiert die Beklagte etwa unter „Einstellungen zum Datenschutz" (Anlage K 59) mit: „Wir tauschen

Daten mit Drittanbietern aus, die uns helfen, unser Werbeangebot zu verbessern, zu finanzieren sowie personalisierte Inhalte darzustellen. Hierfür werden von uns und unseren Partnern Technologien wie Cookies verwendet. […]“. Infolge dieses Austausches mit Drittanbietern (Vendoren) kommt es - jedenfalls nach Einwilligungserteilung - auch zu der von dem Kläger weiter angegriffenen Setzung von Third-Party-Cookies durch diese. Soweit die Beklagte hierzu ausführt, nicht sie, sondern die Dritten würden solche Cookies auf dem Endgerät speichern, dringt sie hiermit nicht durch. Denn durch die Einbindung der CMP auf der Webseite der Beklagten und die hierauf fußende Übersendung des TC-Strings und die darin enthaltende Zustimmung des Nutzers ist es gerade die Beklagte, welche eine solche Cookie-Setzung durch Dritte veranlasst und ermöglicht. So wurde der Webseitenbetreiber („Publisher“) auch in der Entscheidung der belgischen Datenschutzbehörde als datenschutzrechtlicher Verantwortlicher (a.a.O., S. 84 ff., Rn. 387 ff.) gesehen.

107
v) Ausweislich der von der Beklagten mittels der CMP erteilten Informationen und der oben festgestellten Vorgänge dient der beanstandete Einsatz der Cookies, insbesondere des TC Strings, der Erstellung von Nutzerprofilen zum Zwecke der domainübergreifenen Nachverfolgung des jeweiligen Nutzers zu Werbezwecken im TCF 2.0-Netzwerk.

108
d) Die Speicherung des streitgegenständlichen Cookies im Rahmen des TFC 2.0 Netzwerks erfolgt auch nicht mit wirksamer Einwilligung der Endnutzer. Insbesondere ist die Information des Endnutzers und die Einwilligung nicht gemäß der Verordnung (EU) 2016/679 erfolgt, § 25 Abs. 1 S. 2 TTDSG.

109
§ 25 Abs. 1 S. 2 TTDSG verweist sowohl bezüglich der Informationspflichten als auch der formalen und inhaltlichen Anforderungen an eine Einwilligung auf die DSGVO (vgl. BT-Drs. 19/27441, 38). Die Anforderungen an eine wirksame Einwilligung ergeben sich damit aus Art. 7 und Art. 8 DSGVO. Für die Beurteilung der Wirksamkeit einer Einwilligung gemäß § 25 Abs. 1 S. 1 TTDSG sind demnach im Wesentlichen dieselben Bewertungsmaßstäbe anzulegen, wie bei einer Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO (MAH GewRS, a.a.O. Rn. 132; vgl. auch OH Telemedien 2021, S. 10 ff.). An diesem Prüfungsmaßstab ändert auch der Umstand nichts, dass der Kläger die Klage ausdrücklich allein auf das TTDSG und nicht auf Verstöße gegen die DSGVO stützt. Denn vorliegend ist die DSGVO lediglich Prüfungsmaßstab für die tatbestandlichen Voraussetzungen des § 25 TTDSG kraft der ausdrücklichen gesetzlichen Verweisung in Abs. 1 S. 2 (anders allerdings bei den Klageanträgen Nr. 2 und 3, siehe hierzu unter Ziffer II. und III.).

110
i) Einwilligung im Sinne des Art. 4 Nr. 11 DSGVO ist 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.

111
Die vorliegend von der Beklagten eingeholte Einwilligung beruht bereits nicht auf einer freiwilligen Entscheidung der Nutzer (so auch BayLDA, Stellungnahme vom 09.09.2022, S. 9 ff., Bl. 654 ff. d.A.):

112
Als freiwillig kann die Einwilligung nur dann betrachtet werden, wenn die betroffene Person tatsächlich eine Wahlmöglichkeit hat, d.h. auch ohne Nachteile auf die Erteilung der Einwilligung verzichten kann (Ehmann/Selmayr/Klabunde, 2. Aufl. 2018, DSGVO Art. 4 Rn. 49). Dies ist angesichts des Aufbaus der von der Beklagten verwendeten CMP nicht der Fall. So kann auf der ersten Seite der CMP (vgl. Anlage K 58), welche die Nutzung der Webseite bis zur Einwilligungserteilung oder -verweigerung durch teilweises Verdecken der Webseite verhindert, lediglich die Einwilligung in vollem Umfang erteilt oder durch Betätigung der Schaltfläche „Einstellungen“ eine gesonderte Auswahl getroffen werden. Dabei ist die Schaltfläche „Akzeptieren“ nochmals durch die blaue Markierung besonders in den Vordergrund gerückt, so dass für den Nutzer offensichtlich ist, dass deren Betätigung die schnellste Möglichkeit darstellt, die Webseite zu nutzen. Bereits der Umstand, dass ein Besucher die Webseite der Beklagten nicht ohne weitere Interaktion mit der CMP nutzen kann, spricht gegen eine freiwillige Entscheidung. Zudem ist auf der ersten Ebene der CMP allein aus dem Fließtext ersichtlich, dass die Einwilligung auch abgelehnt werden kann. Ob eine Ablehnung

mit Nachteilen oder Mehraufwand verbunden ist, kann der Nutzer dagegen nicht erkennen. Jedenfalls ist eine Verweigerung der Einwilligung erst nach Betätigung der Schaltfläche „Einstellungen“ auf einer zweiten Ebene der CMP möglich und damit mit mehr Aufwand als das bloße „Akzeptieren“ der Datenverarbeitung verbunden. Zwar erscheint der damit beschriebene Aufwand als verhältnismäßig gering. Gleichwohl ist ein solcher zusätzlicher Aufwand angesichts der im Internet gerade üblichen Schnelligkeit und geringen Aufmerksamkeit der Nutzer nicht unerheblich. Dabei ist ferner zu berücksichtigen, dass auf der zweiten Ebene der CMP die Vielzahl von Einstellungsmöglichkeiten zu einer weiteren Erschwerung der Einwilligungsverweigerung führt. Denn auch hier wird wiederum die Schaltfläche „Alle Akzeptieren“ sowohl aufgrund der farblichen Gestaltung als auch durch ihre Positionierung und Größe nochmals hervorgehoben, während die Schaltfläche „alle ablehnen“ in Größe und Gestaltung dagegen unauffällig gehalten ist. Eine sachliche Rechtfertigung für die unterschiedliche Behandlung der Wahlmöglichkeiten „Einwilligung erteilen“ und „Einwilligung verweigern“ ist weder vorgetragen noch ersichtlich. Angesichts der unterschiedlichen Gestaltung erscheint es daher naheliegend, dass hierdurch das Wahlrecht der Webseitenbesucher beeinflusst werden soll (vgl. BGH NJW 2020, 2540 Rn. 37 - Planet 49). Keine Rolle spielt es in diesem Zusammenhang, dass die Beklagte die CMP als Teil des TFC 2.0 einsetzt und behauptet, diesbezüglich keine Gestaltungsmöglichkeiten zu haben. Denn die Beklagte ist dafür selbst verantwortlich, eine freiwillige und damit wirksame Einwilligung einzuholen.

113
ii) Ob die Einwilligung daneben auch wegen Verstoßes gegen die (gesetzlich nicht geregelten) Informationspflichten (vgl. hierzu etwa EuGH MMR 2019, 732 Rn. 75 - Planet49) unwirksam ist - wofür angesichts des bloßen Umfangs der dargelegten Verarbeitungsvorgänge und des im CMP verwendeten Aufbaus mittels Menüs und Untermenüs erhebliche Gründe sprechen - kam es daher im Ergebnis nicht mehr an.

114
iii) Mangels Wirksamkeit einer etwaigen Einwilligung konnte es dahinstehen, ob - wie vom Kläger behauptet (siehe Vortrag zu Third-Party-Cookies des Werbenetzwerkes Criteo) - trotz Einwilligungsverweigerung Cookies auf dem Endgerät des Nutzers gespeichert werden.

115
e) Die Einwilligung war schließlich auch nicht gem. § 25 Abs. 2 TTDSG entbehrlich, insbesondere war die Speicherung oder der Zugriff auf Informationen nicht unbedingt erforderlich ist, damit der Anbieter eines Telemediendienstes einen vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann, § 25 Abs. 2 Nr. 2 TTDSG. Unbedingt erforderlich ist in diesem Sinne nur, was technisch notwendig ist (vgl. BT-Drs. 19/27441, 38). Es kommt mithin auf den Verwendungszweck bzw. den Dienst an, der gegenüber dem Nutzer erbracht werden soll (MAH GewRS, § 27 Rn. 131). Die streitgegenständlichen Cookies, die der domainübergreifenden Nachverfolgung zu Analyse- und Marketingzwecken dienen, sind für den Betrieb eines Nachrichtenportals nicht technisch unbedingt erforderlich (vgl. Golland, Das Telekommunikation-Telemedien-Datenschutzgesetz, Cookies und PIMS als Herausforderungen für Website-Betreiber, NJW 2021, 2238). Dies entspricht auch der Rechtslage zu § 15 Abs. 3 S. 1 TMG, zu dem BGH in richtlinienkonformer Auslegung bereits festgestellt hat, dass eine Zustimmung jedenfalls bei Einsatz von Cookies zur Erstellung von Nutzerprofilen für Zwecke der Werbung und Marktforschung erforderlich ist (BGH ZD 2020, 467 Rn. 47 ff. - Cookie-Einwilligung II). Allein der Umstand, dass die Datenspeicherung der Finanzierung des Angebotes der Beklagten dient oder im Rahmen des TCF 2.0 vorgegeben ist, kann hierfür nicht genügen. Es handelt sich dabei lediglich um subjektive Interessen der Beklagten. Im Übrigen ist die Vorschrift als Ausnahme vom Grundsatz der Einwilligungsbedürftigkeit nach allgemeinen Grundsätzen eng auszulegen.

116
Für eine Entbehrlichkeit der Einwilligung aufgrund von § 25 Abs. 2 Nr. 1 TTDSG liegen die Voraussetzung ersichtlich nicht vor, bzw. sind solche auch nicht vorgetragen.

117
4. Soweit der Kläger weitere Verstöße der Beklagten gegen § 25 TTDSG durch unterschiedliche von dieser verwendete Technologien behauptet, folgt die Kammer dem nicht. Insofern fehlt es an entsprechend substantiiertem Vortrag zu entsprechenden Verletzungshandlungen der Beklagten bzw. unterfallen die behaupteten Verstöße nicht dem Klageantrag.

118
a) Der Kläger beanstandet unter anderem ausdrücklich den Einsatz von „Google Analytics“-Cookies mit der Bezeichnung „_gat_UA-89731071-12“, „_ga“ und „gid“, welche von der Beklagten zur domainübergreifenden Nachverfolgung (u.a. durch Einsatz eines JavaScripts „linkid.js“) eingesetzt werden würden. Die Beklagte hat dies jedoch substantiiert bestritten, indem sie darlegt, dass sie „GoogleAnalytics“ nur in einer reduzierten Form verwendet und auch der Einsatz des Plugins „linkid.js“ nur der optimierten Linkzuordnung innerhalb der Domain diene, mithin kein domainübergreifendes Tracking ermögliche. Die Beklagte ist damit ihrer sekundären Darlegungslast nachgekommen. Demgegenüber hat der Kläger für seine Behauptung nicht Beweis angeboten.

119
Die Kammer geht zwar auch beim Einsatz der oben beschriebenen Cookies von einem Verstoß gegen § 25 TTDSG aus, da hierfür eine Speicherung auf dem Endgerät des Nutzers ohne wirksame Einwilligung genügt. Die Kammer kann allerdings auf Grundlage des Parteivortrags und der Beweisangebote nicht feststellen, dass die oben beschriebenen Cookies tatsächlich im Sinne des Klageantrags der domainübergreifenden Aufzeichnung und Auswertung des Nutzerverhaltens zu Analyse- und Marketingzwecken dienen.

120
Entsprechendes gilt für den von dem Kläger behaupteten Einsatz eines Tracking-Programcodes „Google AMP Client ID“ mit dem Zweck eines domainübergreifenden Trackings. Auch hier hat die Beklagte den Einsatz zum domainübergreifenden Tracking substantiiert bestritten.

121
b) Aus dem klägerischen Vortrag zu von der Webseite der Beklagten ausgehenden „HTTP-Transaktionen“ geht bereits nicht hervor, dass diese für sich genommen, also ohne Verknüpfung mit Cookies, dem § 25 TTDSG bzw. dem Klageantrag unterfallen. Insbesondere fehlt es an der substantiierten Darlegung, dass diese Transaktionen zu einer Speicherung auf dem Endgerät des Nutzes führen bzw. solche gespeicherten Informationen abrufen. Auch ein in diesem Zusammenhang erfolgendes domainübergreifendes „Tracking“ ist nicht ausreichend dargelegt.

122
c) Gleiches gilt für die vom Kläger beanstandete Nutzung des „Local- und Session Storage“. Auch hier ist nicht ersichtlich, inwiefern diese Technik von der Beklagten konkret für eine domainübergreifenden Nachverfolgung genutzt wird.

123
II. Hinsichtlich des Klageantrags Nr. 2 und Nr. 3 ist die Klage unbegründet.

124
1. Der Kläger begehrt von der Beklagten mit Klageantrag Nr. 2 ferner auch Unterlassung, wenn sie nicht den Nutzern Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermittelt. Derartige Informationspflichten können sich allein aus der DSGVO ergeben (Art. 12 DSGVO). Zwar sind für den Fall, dass in Telemedien auch personenbezogene Daten verarbeitet werden, auch die Vorgaben der DSGVO zu beachten (MAH GewRS, a.a.O., Rn. 120) Der Kläger hat indessen ausweislich des Protokolls der mündlichen Verhandlung die Klage allein auf TTDSG gestützt. Zwar verweist § 25 TTDSG u.a. auf die Verordnung (EU) 2016/679 und damit auf die DSGVO (siehe oben). § 25 TTDSG hat jedoch die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder den Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, zum Gegenstand und sieht hierfür ein Verbot mit Erlaubnisvorbehalt vor. Eine über den Wortlaut des § 25 TTDSG hinausgehende Informationspflicht kann der Kläger daher nicht gesondert geltend machen, ohne sich zugleich kumulativ auf die DSGVO zu stützen. Mangels Anspruchsgrundlage nach dem TTDSG war die Klage daher insoweit abzuweisen.

125
2. Auch der Klageantrag Nr. 3, der für den Falle der gemeinsamen Verantwortlichkeit eine Unterlassung zum Gegenstand hat, soweit nicht entgegen Art. 26 Abs. 2 S. 2 DSGVO das Wesentliche der Vereinbarung zwischen gemeinsam für die Verarbeitung Verantwortlichen den Nutzern zur Verfügung gestellt wird, ist mangels Anspruchsgrundlage nach dem TTDSG unbegründet (siehe oben unter 1.). Denn die Pflichten bei

der gemeinsamen Verantwortlichkeit (§ 26 Abs. 1 DSGVO) sind vorliegend nicht Gegenstand der Klage, nachdem der Kläger diese auf das TTDSG beschränkt hat. Aus der Verweisung in § 25 Abs. 1 S. 2 TTDSG eine umfängliche Verweisung auf die DSGVO zu entnehmen, ginge zu weit.

126
C. Soweit die Beklagte Antrag auf Vollstreckungsschutz nach § 712 ZPO gestellt hat, war diesem nicht zu entsprechen. Die Voraussetzungen für eine Schuldnerschutzanordnung sind nicht gegeben, insbesondere würde der Beklagten durch die Vollstreckung nicht ein nicht zu ersetzender Nachteil entstehen. So wäre die Beklagte im Falle der Vollstreckung nicht gehalten, ihr Angebot in der jetzigen Form insgesamt einzustellen. Vielmehr wäre es nur erforderlich, dass sie bei der Einwilligungseinholung im Sinne des § 25 TTDSG informiert. Eine solche Informationserteilung erscheint auch nicht unzumutbar. Damit einhergehende Nachteile, z.B. die Kosten der Erstellung einer den gesetzlichen Anforderungen genügenden Informationserteilung, etwa in Form einer angepassten CMP, wären jedenfalls keine „nicht zu ersetzenden“ Nachteile i.S.v. § 712 S. 1 ZPO.

127
D. Soweit die nachgereichten, nicht nachgelassenen Schriftsätze anderes als bloße Rechtsausführungen enthalten, waren sie gemäß § 296a ZPO nicht mehr zu berücksichtigen (vgl. Zöller/Greger, ZPO, 32. Auflage, § 132, Rn. 4), eine Wiederöffnung der Verhandlung nach § 156 ZPO war, auch in Bezug auf den nachgelassenen Schriftsatz der Beklagten vom 09.09.2022 (Bl. 637/645 d.A.), nicht geboten (vgl. auch BGH NJW 2000, 143 f. und Zöller/Greger, 32. Auflage, § 156, Rn. 4 und 5).

128
E. Die Kostenentscheidung beruht auf § 92 Abs. 1 ZPO, soweit der Kläger mit seinen Klageanträgen Nr. 2 und Nr. 3 unterliegt. Soweit der Kläger durch seine Klageänderungen (siehe oben unter A.I.) sein ursprüngliches Begehren nicht mehr weiterverfolgt hat, ist ihm der hierauf entfallende Anteil entsprechend § 269 Abs. 3 S. 2 ZPO aufzuerlegen (vgl. BeckOK ZPO/Bacher, 46. Ed. 01.09.2022, ZPO § 263 Rn. 36). Aufgrund des Austausches des Streitgegenstands sowohl im Hinblick auf die datenschutzrechtlichen Vorschriften als auch im Hinblick auf die von der Beklagten verwendete Einwilligungs-Software gewichtet die Kammer ein entsprechendes Unterliegen mit 50 % und das insgesamte Unterliegen mit 75 %.

129
F. Die Entscheidung zur vorläufigen Vollstreckbarkeit beruht auf § 709 S. 1 und 2 ZPO.