Yannick Häntzschel

Real-Time-Bidding – Die Vermarktung von Werbeflächen im Internet

„Alle akzeptieren“ – ein Button, den wohl die meisten von uns regelmäßig betätigen, um störende Pop-Ups loszuwerden. Doch was akzeptieren wir da eigentlich? Dieser Beitrag beschäftigt sich mit einem Vertriebssystem für Werbeflächen, das in der breiten Bevölkerung kaum bekannt ist und doch nahezu jeden von uns betrifft: dem Real-Time-Bidding. Im Zentrum steht eine Entscheidung der belgischen Datenschutzaufsicht, die im Februar 2022 für Aufruhr in der Branche gesorgt hat. Sie wirft grundsätzliche Rechtsfragen zur Zulässigkeit von Datenverarbeitungen in Real-Time-Bidding Systemen auf – Rechtsfragen, die aktuell auf eine Beantwortung durch den EuGH warten. Neben einer grundlegenden Erläuterung, wie das Real-Time-Bidding funktioniert, soll dieser Beitrag in erster Linie ein Verständnis dafür schaffen, warum diese Rechtsfragen elementar für Nutzer:innen und Industrie sind und sich mit den Ausführungen der belgischen Behörde kritisch auseinandersetzen.

Entscheidungsbesprechung Autorité de protection des données vom 2. Februar 2022, DOS-2019-01377

I. Einleitung

Personalisierte Werbung ist ein Geschäftsmodell, das immer wieder wegen massenhafter Verarbeitung von personenbezogenen Daten in Kritik gerät. Als besonders problematisch wird das „Tracking“ gesehen: das Erstellen von detaillierten Nutzerprofilen, die genutzt werden, um Nutzer:innen maßgeschneiderte Werbeanzeigen zu präsentieren.[1] Bei vielen Nutzer:innen führt der Gedanke, dass Unternehmen umfangreiche Datensätze über das eigene Verhalten im Internet anlegen, zu einem gewissen Unwohlsein. Doch wird damit auch gegen geltendes Recht verstoßen? Im Folgenden soll ein besonders kontroverses Vermarktungssystem betrachtet werden: das Real-Time-Bidding (RTB).

1 Vgl. etwa die „Tracking-Free Ads Coalition” des EU-Parlaments (1. Mai 2023).

1. Werbeplatzierung in Medien

Um eine Bewertung von RTB-Systemen aus rechtlicher Sicht vorzunehmen, sollen zunächst die teilnehmenden Parteien und Prozesse in RTB-Systemen erläutert werden.

a. Parteien

Folgende Parteien nehmen an RTB-Systemen typischerweise teil:

a) Nutzer:innen: Die Endnutzer:innen, die das Ziel der Werbeanzeigen sind.
b) Publisher: Die Betreiber:innen der Medien, die von Nutzer:innen genutzt werden und deren Werbeflächen verkauft werden.
c) Werbetreibende (engl. „advertisers“): Akteure, die ihre Werbung einer möglichst relevanten Zielgruppe (z.B. von möglichen Kund:innen) präsentieren wollen.
d) Sell-Side-Platform (SSP): Plattformen, die Publisher bei der Vermarktung ihrer Werbeflächen unterstützen und eine Aufforderung auf diesen Platz zu bieten (Bid-Request) senden.
e) Demand-Side-Platform (DSP): Plattformen, die den Kauf von Werbeflächen für Werbetreibende unterstützen.
f) AdExchange: Eine Plattform, die zwischen Demand-Side und Supply-Side vermittelt und als Schnittstelle eine Kommunikation erlaubt.
g) Data-Management-Platform (DMP): Plattformen, die aus zahlreichen Quellen große Mengen an Nutzer-Daten sammeln, kategorisieren, verwalten und zu Nutzerprofilen zusammenfassen, um Werbetreibenden eine noch zielgerichtetere

Werbung zu ermöglichen.
h) Vendoren: SSPs, DSPs, Ad Exchanges, Werbetreibende und DMPs. [2]

Bei der gehandelten Ware in RTB-Systemen handelt es sich nicht um die Werbung (oder das beworbene Produkt), sondern um die Werbefläche. Der Publisher ist damit ebenso wie die SSP der „Supply-Side" der Anbieterseite zuzuordnen, während DSP und Werbetreibende die „Demand-Side" also die Nachfrageseite bilden.

b. Abläufe

Der Vorgang kann folgendermaßen beschrieben werden: [3]

1. Ein:e Nutzer:in ruft die Website des Publishers auf. Dabei werden vorhandene Cookie-Daten (siehe A.III.) und weitere beim Aufrufen übermittelte Daten (siehe A.II.) der:des Nutzer:in vom Publisher ausgelesen.
2. Die vorhandenen Daten der:des Nutzer:in werden vom Publisher an die SSP übermittelt.
3. Die SSP fasst die vorhandenen Daten zu einem Bid-Request für diese:n konkrete:n Nutzer:in zusammen. Über die Ad-Exchange wird der Bid-Request mit kooperierenden DSPs geteilt.
4. Über die Ad-Exchange kann der DSP die Möglichkeit eingeräumt werden, die im Bid-Request vorhandenen Daten mit Daten anzureichern, die eine DMP bereits über die:den Nutzer:in hält.
5. Die durch die DSP vertretenen Werbetreibenden geben in Echtzeit Gebote für das Nutzerprofil ab. Die Höhe des Gebotes ist u.a. dadurch bestimmt, wie gut das Nutzerprofil der Zielgruppe des Werbetreibenden entspricht.
6. Der Werbetreibende mit dem höchsten Gebot erhält den Zuschlag und übermittelt dem Publisher die gewünschte Werbeanzeige, um sie der:dem Nutzer:in anzuzeigen (etwa ein Bild oder Video).

2 Entscheidung der belgischen Datenschutzaufsicht APD v. 2. Februar 2022, DOS-2019-01377, nichtoffizielle englische Übersetzung aus niederländischer Sprache (1. Mai 2023, folgend: APD-Entscheidung) Rn. 24 ff. Die in der Entscheidung referierten Erkenntnisse zu technischen Hintergründen von RTB-System stützen sich auf den „Technical Analysis Report of the Inspection Service" vom 6. Januar 2020.

3 Vereinfachte Darstellung in Anlehnung an Darstellungen des Investigation Service, APD-Entscheidung Rn. 27.

2. Der Bid-Request

Im Zentrum dieser Vorgänge steht der sogenannte „Bid-Request", also die Aufforderung Gebote abzugeben. Neben allgemeinen Informationen über den angebotenen Werbeplatz können Bid-Requests auch ein breites Portfolio an Daten über Nutzer:innen enthalten, denen die Werbung angezeigt werden soll. Beispiele für im Bid-Request enthaltene Daten sind: URL/Katergorie der Website; Betriebssystem/Hersteller des Endgeräts; Geographiedaten (z.B. PLZ); Geburtsjahr/Geschlecht der:des Nutzer:in; Interessen der:des Nutzer:in (basierend auf dem Online-Verhalten); Nutzer:in-spezifischer Identifier.[4]

3. Cookies

In diesem Zusammenhang wird ebenfalls die Nutzung von „Cookies" relevant. Hinter diesem Begriff verbirgt sich eine Datei, die auf dem Endgerät der:s Nutzer:in gespeichert wird. Welche Informationen im Cookie gespeichert sind, wer es schreibt und wer es wieder auslesen kann, ist von der Art des Cookies abhängig. Unterschieden wird hier zwischen First-Party-Cookies und Third-Party-Cookies.[5]

a. First-Party-Cookies

Wie der Name suggeriert, ist bei First-Party-Cookies neben den Nutzer:innen, auf deren Endgerät das Cookie gespeichert wird, eine weitere Partei involviert. Dies ist in der Regel der Publisher, der eine Website oder App betreibt, die die Nutzer:innen besuchen bzw. nutzen. Sobald Nutzer:innen die Website aufrufen, senden sie ebenfalls Daten an den Publisher, die es diesem ermöglichen, die Website ordnungsgemäß darzustellen. Dazu gehören etwa Bildschirmgröße, Betriebssystem und Standort (insbesondere bei mehrsprachigen Angeboten). Zur Vereinfachung dieser Prozesse speichert der Publisher die ihm übermittelten Daten in einer Datei auf dem Endgerät des Nutzers – dem Cookie. Die dort gespeicherten Daten kann er beim nächsten Aufruf der Seite wieder auslesen und nutzen. Allgemein dienen First-Party-Cookies

4 APD-Entscheidung Rn. 29.

5 *Specht,* Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 9 Rn. 63.

in erster Linie dazu, das Nutzer:innenerlebnis zu optimieren und Informationen, die Nutzer:innen einmal senden, bei zukünftigen Besuchen wiederverwenden zu können. Weitere Beispiele sind ein Einkaufskorb bei Online-Shops, Benutzer:innennamen/Passwörter und allgemeine Website-Einstellungen.

b. Third-Party-Cookies

Deutlich interessanter für AdTech[6] Anbieter:innen sind Third-Party-Cookies. Hier wird das Cookie nicht vom Publisher gesetzt, sondern von einer dritten Partei – regelmäßig einem Akteur in RTB-Prozessen. Entscheidend ist, dass dieser Dritte das Cookie nicht nur setzt, sondern es auch später wieder auslesen kann. Da er die Cookies nicht nur für einen Publisher setzt, sondern für ein ganzes Portfolio an Websites und anderen Medien, ermöglichen es Third-Party-Cookies, umfangreiche Profile über das Nutzer:innenverhalten zu erstellen. Diese Profile können anschließend genutzt werden, um eine gezielte Platzierung von Werbung bei diesen Nutzer:innen an Werbetreibende zu vermarkten.[7]

II. Marktstandards: TCF & OpenRTB

Bereits jetzt wird ersichtlich, dass RTB-Systeme umfangreiche Datenverarbeitungsprozesse mit tausenden von Beteiligten beinhalten. Es stellt sich also die Frage, wie diese Prozesse nicht nur technisch ermöglicht werden können, sondern darüber hinaus auch die Einhaltung einschlägiger Regulatorik sichergestellt werden kann. Die Antwort der Industrie auf diese Frage lautet: Standards.

Standards sind in industriellen Anwendungen insbesondere dort allgegenwärtig, wo viele Parteien zusammenarbeiten müssen. Anstelle von aufwändiger Individualkommunikation wird ein gemeinsamer Nenner entwickelt, der für alle nutzbar ist. Ein prominentes Beispiel ist etwa der Bluetooth-Standard, der eine kabellose Verbindung von Geräten zahlreicher Hersteller ermöglicht.[8]

Derartige Standards existieren auch für RTB-Prozesse. Neben dem Authorized Buyers Protokoll, herausgegeben von Google[9], sind dies etwa das OpenRTB Protokoll, herausgegeben durch das IAB Technology Lab[10], und das Transparency & Consent Framework (TCF), herausgegeben durch IAB Europe[11]. Im Folgenden sollen sich die Ausführungen auf die beiden letztgenannten Standards beschränken.

1. Unterschiede

Wichtig ist dabei zunächst eine Abgrenzung beider Standards voneinander. Das OpenRTB Protokoll ist ein technischer Standard, der eine Kommunikation zwischen unterschiedlichen Akteur:innen im RTB-System ermöglichen und damit die Funktionalität sicherstellen soll. Dafür bedient er sich unter anderem technischer Spezifikationen, wie einem Application Programming Interface (API): einer Schnittstelle, die es Programmier:innen ermöglicht an ein fremdes System anzuknüpfen.[12]

2. Transparency & Consent Framework

Demgegenüber soll das TCF den Teilnehmenden die Einhaltung der einschlägigen Regulatorik ermöglichen, namentlich der Verordnung (EU) 2016/679 (DSGVO). Problematisch sind im Kontext von RTB-Systemen regelmäßig die Rechtsgrundlage für eine Verarbeitung von personenbezogenen Daten (Art. 6 I DSGVO) und die Erfüllung von Transparenzpflichten (Art. 12 ff. DSGVO). Um diesen Anforderungen zu genügen, stellt das TCF einheitliche Vorgaben zu Verarbeitungszwecken auf und setzt sogenannte Consent Management Platforms (CMP) ein, die einen vorgelagerten Zertifizierungsprozess durchlaufen müssen. Die teilnehmenden „Vendoren“ (ein Begriff mit dem in

6 Der Begriff AdTech leitet sich von dem englischen Begriff „Advertising Technology“ ab und bezeichnet allgemein Technologie (z.B. Software oder Analysewerkzeuge), die für Werbezwecke eingesetzt wird.

7 Difference Between First-Party and Third-Party Cookies (1. Mai 2023).

8 Bluetooth Technologie-Übersicht (1. Mai 2023).

9 Authorized Buyers–Übersicht (1. Mai 2023).

10 *IAB Technology Laboratory,* Real Time Bidding (RTB) Project (1. Mai 2023).

11 TCF – Transparency & Consent Framework v2.0 (1. Mai 2023).

12 TCF – Transparency & Consent Framework (1. Mai 2023).

Rahmen des TCF die Werbetreibenden, SSP, DSP, Ad Exchange und DMP zusammengefasst werden) sind darüber hinaus in einer „Global Vendors List" öffentlich einsehbar (aktuell 818 Unternehmen).[13] Die Publisher können dabei wählen, welche Verwendungszwecke sie den Vendoren anbieten möchten.

3. Consent Management Platforms

Eine besondere Rolle für die DSGVO-Compliance kommt dabei den CMP zu. Sie sind dafür verantwortlich, Nutzer:innen über die Datenverarbeitungen mit allen verbundenen Transparenzpflichten aufzuklären und eine notwendige Einwilligung einzuholen. Der dahinterliegende Prozess kann folgendermaßen beschrieben werden:

1. Sobald ein:e Nutzer:in das Medium (bspw. die Website) aufruft, sendet die CMP ein Pop-Up (z.B. in Form eines Cookie-Banners), das der:dem Nutzer:in in die Website eingebettet präsentiert wird.
2. In diesem Pop-Up werden der:dem Nutzer:in Informationen über die beteiligten Vendoren und die gewählten Verarbeitungszwecke dargestellt.
3. Die:Der Nutzer:in kann nun Einstellungen vornehmen und für die einzelnen Vendoren und Verarbeitungszwecke ihre:seine Einwilligung erteilen oder verweigern und bei berechtigtem Interesse als Rechtsgrundlage für die Verarbeitung von ihrem:seinem Widerspruchsrecht Gebrauch machen. Üblicherweise steht der:dem Nutzer:in auch die Option zur Verfügung, pauschal allen Zwecken und Vendoren zuzustimmen.
4. Die von der:dem Nutzer:in gewählten Einstellungen – also die erteilen Zustimmungen und Widersprüche (im Folgenden „Nutzer:in-Präferenzen") – werden in einer Datei zusammengefasst: dem TC-String. Dabei handelt es sich um eine Textdatei, deren konkrete Zusammensetzung durch den standardisierten Aufbau den teilnehmenden Vendoren die Nutzer:in-Präferenzen mitteilt.
5. Der TC-String wird im Anschluss als Cookie auf dem Endgerät der:des Nutzer:in gespeichert und kann bei zukünftigen Besuchen des Mediums weiterverwendet werden.[14]

13 Vendor List TCF 2.0 (1. Mai 2023).
14 APD-Entscheidung Rn. 41 ff.

III. Die Entscheidung der belgischen Aufsichtsbehörde vom 2. Februar 2022

Kritik an diesem System wurde kürzlich an die zuständige belgische Datenschutzaufsicht Autorité de protection des données (APD) herangetragen, deren Litigation Chamber (die Streitbeilegungsstelle der APD, folgend: Kammer) am 2. Februar 2022 eine Entscheidung zu den Beschwerden veröffentlichte. Gegenstand der Entscheidung ist die Verarbeitung von personenbezogenen Daten im Rahmen des TCF. Diese Abgrenzung hat entscheidende Auswirkungen auf die Reichweite der Entscheidung. Wie bereits dargestellt, ist das TCF dazu gedacht, DSGVO-Compliance herzustellen, indem Nutzer aufgeklärt werden und deren Einwilligung als Rechtsgrundlage eingeholt wird. Explizit nicht von der Entscheidung erfasst sei daher der RTB-Prozess selbst und damit auch das OpenRTB-Protokoll.[15] Klar ist allerdings, dass die enge Verflechtung erhebliche Auswirkungen auf angeschlossene RTB-Systeme haben wird.

Im Folgenden sollen vier Kernaussagen der Entscheidung herausgestellt und kritisch besprochen werden.

1. Der TC-String als personenbezogenes Datum

Durch die Eingrenzung auf das TCF stellt sich die Frage, welche personenbezogenen Daten in diesem Rahmen verarbeitet werden, die den Anwendungsbereich der DSGVO überhaupt erst eröffnen. Nach Art. 4 Nr. 1 DSGVO sind personenbezogene Daten *„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen".*

Anders als IAB Europe selbst ist die Kammer der Ansicht, dass der TC-String, in dem die Nutzer:in-Präferenzen festgehalten sind, ein solches personenbezogenes Datum darstellt. Aus Sicht der Kammer sind hierfür zwei Faktoren maßgeblich:

15 APD-Entscheidung Rn. 289.

a. IP-Adresse

Zum einen erlaube die Verknüpfung des TC-Strings mit der IP-Adresse von Nutzer:innen die Aussonderung einer spezifischen natürlichen Person. Dabei stellt auch die Kammer fest, dass der TC-String allein keine Zuordnung zu einer natürlichen Person erlaubt.[16] Diese Bewertung kann überzeugen, denn auch wenn der TC-String individuelle Nutzer:innenpräferenzen enthält (und damit nahe liegt ihn als „unique identifier" zu bewerten) ist er nicht einzigartig. Sobald mehr als eine Person die gleichen Präferenzen wählt, ist eine eindeutige Zuordnung nicht mehr möglich. Sobald eine CMP aber einer:einem Nutzer:in das Consent-Pop-Up sendet, verarbeitet sie automatisch auch ihre:seine IP-Adresse. Bei Speicherung oder dem späteren Auslesen des TC-String in einem Cookie ist also die Verknüpfung mit der IP-Adresse der:des Nutzer:in durch die CMP möglich. Die Kammer klassifiziert die IP-Adresse auch als personenbezogenes Datum und beruft sich dabei auf Erwägungsgrund 30 der DSGVO.[17] Dieser muss allerdings zwingend in Verbindung mit der Rechtsprechung des EuGH zu der Klassifizierung von IP-Adressen gelesen werden, der lediglich einen relativen Personenbezug feststellt. Voraussetzung ist demnach, dass für mutmaßliche Verantwortliche Möglichkeiten bestehen, diese IP-Adresse einer natürlichen Person zuzuordnen. Dies ist bei IP-Adressen von Privatpersonen nicht ganz unproblematisch. Es handelt sich hier überwiegend um dynamische IP-Adressen. Anders als etwa eine postalische Anschrift ist eine dynamische IP-Adresse nicht dauerhaft einem einzelnen Anschluss zugeordnet. Vielmehr wird die IP-Adresse einem Anschluss lediglich temporär zugeordnet und nach einer gewissen Zeit oder bei neuer Verbindung mit dem Netzwerk (etwa bei Router-Neustart) wieder freigegeben und einem neuen Anschluss zugewiesen.[18] Dass IAB Europe über rechtliche oder tatsächliche Mittel verfügt, um diese Verbindung herzustellen, ist also alles andere als selbstverständlich. Um einen Personenbezug des TC-String über seine Verknüpfung mit der IP-Adresse zu etablieren, bedürfte es also einer tiefergehenden Bewertung, ob bzw. inwieweit IAB Europe über Mittel verfügt, die einen Personenbezug der IP-Adresse begründen würden. Zumindest der Entscheidungsbegründung ist diese Auseinandersetzung jedoch nicht zu entnehmen.

b. Zweck des TC-Strings

Darüber hinaus begründet die Kammer ihre Einordnung mit dem Zweck des TC-Strings. Er dient dazu, die von Nutzer:innen gespeicherten Präferenzen zu einem späteren Zeitpunkt wieder diesen spezifischen Nutzer:innen zuzuordnen. Damit der TC-String diese Funktion erfüllen kann, müsse es also a priori eine Möglichkeit zur Zuordnung zu einer natürlichen Person geben, ergo einen Personenbezug im Sinne der DSGVO.[19] Diese Argumentationslinie wird grundsätzlich auch von der Artikel 29 Arbeitsgruppe geteilt. Bei der Artikel 29 Arbeitsgruppe handelte es sich um ein unabhängiges Expertengremium der Europäischen Kommission, das sich mit Fragen des Schutzes der Privatsphäre und personenbezogener Daten auseinandersetzte. Seit 1997 veröffentlichte die Gruppe regelmäßig unverbindliche Stellungnahmen zu diesen Fragen.[20] Mit Inkrafttreten der DSGVO am 25. Mai 2018 wurde sie durch den Europäischen Datenschutzausschuss (EDSA) abgelöst.[21]

In der Stellungnahme 4/2007 zum Begriff „personenbezogene Daten" äußert sich die Artikel 29 Arbeitsgruppe folgendermaßen:
„In these cases, where the purpose of the processing implies the identification of individuals, it can be assumed that the controller or any other person involved have or will have the means „likely reasonably to be used" to identify the data subject. In fact, to argue that individuals are not identifiable, where the purpose of the processing is precisely to identify them, would be a sheer contradiction in terms".[22]

Es bestehen allerdings Zweifel, ob diese Logik auf den Fall des TCF übertragen werden kann. In dem zitierten Beispiel wird die Identifikation durch Videoaufzeichnungen behandelt. Klar ist, dass

16 APD-Entscheidung Rn. 300.
17 APD-Entscheidung Rn. 303 f.
18 EuGH vom 19.10.2016, Rs. C-582/14 – Breyer, Rn. 36-49.
19 APD-Entscheidung Rn. 310 ff.
20 Opinions and recommendations (9. Juni 2023).
21 Vermächtnis: Artikel 29 der Datenschutzgruppe (9. Juni 2023).
22 *Artikel 29 Gruppe*, WP 136 – Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", S. 16.

diese auch ein personenbezogenes Datum darstellen, wenn keine direkte Identifikation stattfindet. Denn der grundsätzliche Zweck der Aufzeichnung ist es, wenn nötig, eine Identifikation zu ermöglichen. Die Natur dieser Identifikation unterscheidet sich aber grundlegend von der Zuordnung des TC-String zu spezifischen Nutzer:innen. Die Identifikation einer Person anhand von Videoaufzeichnungen ist permanent. Der TC-String wird Nutzer:innen jedoch nur punktuell zugeordnet. Dies bedeutet zwar nicht, dass die Handreichung der Arbeitsgruppe nicht übertragbar ist. Nach hier vertretener Ansicht wäre allerdings eine differenziertere Auseinandersetzung mit den exakten Modalitäten der Zuordnung und Identifizierung erforderlich.

2. Verantwortung

Eine weitere zentrale Feststellung trifft die Kammer mit Blick auf die Verantwortung für die Verarbeitung von personenbezogenen Daten innerhalb des TCF. Um keine regulatorischen Lücken zu erzeugen und Betroffenen eine eindeutige Partei zur Durchsetzung ihrer Rechte zuzuweisen, besteht für jede Datenverarbeitung ein:e Verantwortliche:r (engl. „Controller"), vgl. dazu Erwägungsgrund 74 DSGVO. Andere an der Verarbeitung beteiligte Personen sind regelmäßig lediglich Auftragsverarbeiter, vgl. Art. 28 DSGVO. Angesichts der oft komplexen Fallgestaltungen bei industriellen Datenverarbeitungsprozessen gibt es jedoch eine Ausnahme: Art. 26 DSGVO etabliert die Rechtsfigur der gemeinsamen Verantwortung. Manche Verarbeitungsprozesse mit mehreren Beteiligten sind organisatorisch so aufgebaut, dass die Verantwortung nicht einem einzelnen Controller zugewiesen werden kann. In diesen Fällen sind die Parteien gemeinsam verantwortlich (Joint Controller). Erforderlich ist aber auch hier eine klare Aufteilung der Verantwortung unter den Controllern, Art. 26 I 2 DSGVO.

Da sich die Rechtsposition von Auftragsverarbeiter und Controller grundsätzlich unterscheiden, ist ein Abgrenzungsmaßstab erforderlich. Art. 4 Nr. 7 DSGVO sagt hierzu aus: wer über die Zwecke und Mittel der Verarbeitung entscheidet, ist nicht nur Auftragsverarbeiter, sondern selbst Controller. Präzisere Abgrenzungskriterien hat der EDSA entwickelt. Demnach muss gefragt werden: *„Warum findet diese Verarbeitung statt?" und „Wer hat beschlossen, dass die Verarbeitung für einen bestimmten Zweck erfolgen sollte?"*[23]

Diese Abgrenzung wird durch die Kammer auch in der genannten Entscheidung durchgeführt. Erforderlich ist sie, weil selbst bei einer Einordnung des TC-String als personenbezogenes Datum IAB Europe diesen selbst nicht direkt verarbeitet, sondern die CMPs und später die Vendoren. Damit die mit der Controller-Stellung verbundenen Pflichten auch auf IAB Europe Anwendung finden, muss etabliert werden, dass IAB Europe über Zwecke und Mittel der Verarbeitung entscheidet.

a. Zwecke

Es ist also eine Bewertung erforderlich, inwiefern IAB Europe durch die Herausgabe und Entwicklung des TCF, Einfluss auf die Zwecke der in diesem Kontext durchgeführten Datenverarbeitungen hat. Spezifisch ist dies die Verarbeitung der Nutzer:innen-Präferenzen in Form des TC-Strings. Neben den festgelegten Verarbeitungszwecken, für die diese Präferenzen abgefragt werden, enthält das TCF auch Vorschriften für die teilnehmenden Organisationen: die „IAB Europe Transparency & Consent Framework Policies"(TCF Policies). In diesen Vorschriften wird auch der Zweck des Netzwerks festgehalten – die Compliance mit einschlägiger Regulatorik, unter anderem durch Information der Nutzer:innen über Verarbeitungszwecke und die Weitergabe der Nutzer:innen-Präferenzen.[24] In diesem Kontext referiert die Kammer auf Aussagen von IAB Europe selbst über die Aufgabe des TC-Strings:

"A TC-String's primary purpose is to encapsulate and encode all the information disclosed to a user and the expression of their preferences for their personal data processing under the GDPR. [...] Vendors decode a TC String to determine whether they have the necessary legal bases to process a user's personal data for their purposes."[25]

23 *EDSA*, Leitlinien 07/2020 Rn. 20 ff.
24 APD-Entscheidung Rn. 334.
25 APD-Entscheidung Rn. 335.

Daraus schließt die Kammer, dass der Zweck des TC-Strings maßgeblich durch IAB Europe bestimmt wird. Darüber hinaus sieht die Kammer auch einen Einfluss auf die nachgelagerte Verarbeitung des TC-Strings in RTB-Systemen. Zwar sei hier zwischen den Zwecken der Verarbeitung des TC-Strings und den Zwecken der Verarbeitung außerhalb des TCF (etwa als Bid-Request) zu differenzieren. Doch werde das TCF angeboten, um das OpenRTB-Protokoll indirekt zu fördern und IAB Europe nehme hier eine Scharnierfunktion ein. Diese Funktion drücke sich auch in der abschließenden Liste an möglichen Verarbeitungszwecken aus, die Vendoren im TCF nutzen können. Hieraus schließt die Kammer einen Einfluss auf Zwecke der Verarbeitung des TC-Strings im Kontext des TCF.[26]

b. Mittel

Bei den Mitteln der Verarbeitung verweist die Kammer in erster Linie auf die technischen Vorgaben, die durch IAB Europe für das TCF vorgegeben werden. Unter anderem nennt die Kammer die CMP API und Vorgaben zur Generierung des TC-Strings.[27] Rechtlich stützt sich die Kammer dabei auf die Wirtschaftsakademie-Rechtsprechung des EuGH.[28] Hier wurde entschieden, dass der Betreiber einer Facebook-Fanpage zusammen mit Facebook Joint Controller ist, wenn er *„durch die von ihm vorgenommene Parametrierung u. a. entsprechend seinem Zielpublikum sowie den Zielen der Steuerung oder Förderung seiner Tätigkeiten an der Entscheidung über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten der Besucher seiner Fanpage beteiligt ist“.*[29]

c. Joint Controller: Vendoren

Mit der Einstufung von IAB Europe als Controller stellt sich ebenfalls die Frage nach der Rolle der übrigen Beteiligten, der Vendoren. Wie bereits ausgeführt, ist es möglich, dass es für eine Verarbeitung mehrere Controller gibt. Der EDSA führt hierzu aus, dass Zwecke und Mittel sowohl durch gemeinsame Entscheidungen der in Frage stehenden Parteien bestimmt werden können als auch durch unterschiedliche aber sich ergänzende Entscheidungen.[30] Hierzu stellt die Kammer zum einen fest, dass die teilnehmenden Organisationen (CMPs, Publishers und AdTech Vendoren) aufgrund ihrer jeweiligen Rollen zu unterschiedlichen Zeitpunkten der Verarbeitung des TC-String auch Joint Controller für diese Datenverarbeitungen sind. Die Kammer geht jedoch noch weiter. Zwar seien TCF und OpenRTB-Protokoll laut IAB Europe unabhängige Systeme. Doch kommt die Bewertung der Kammer zu dem Ergebnis, dass die Systeme so eng aufeinander ausgerichtet seien, dass die Entscheidungen, die IAB Europe durch seine TCF-Policies und technische Spezifikationen getroffen hat auf der einen Seite und die Entscheidungen bezüglich Zweck und Mittel der anschließenden Verarbeitung von personenbezogene Daten durch die teilnehmenden Organisationen in OpenRTB-Protokoll auf der anderen Seite als sich ergänzende Entscheidungen zu sehen sind. Im Ergebnis führe dies dazu, dass IAB Europe zusammen mit den teilnehmenden Organisationen nicht nur für die Verarbeitung der personenbezogenen Daten im TC-String gemeinsam verantwortlich sei, sondern auch für die nachgelagerte Verarbeitung von personenbezogenen Daten (etwa in einem Bid Request).[31]

3. Rechtsgrundlage für Verarbeitung des TC-Strings

Mit der Einstufung des TC-String als personenbezogenes Datum stellt sich ebenfalls die Frage nach der Rechtsgrundlage für dessen Verarbeitung. Gemäß Art. 6 I DSGVO sind mögliche Rechtsgrundlagen: die Einwilligung der betroffenen Person, die Erfüllung eines Vertrages, eine rechtliche Verpflichtung, der Schutz lebenswichtiger Interessen, die Wahrnehmung öffentlicher Aufgaben und ein berechtigtes Interesse. In Frage kommen hier grundsätzlich zwei: Einwilligung und berechtigtes Interesse.

26 APD-Entscheidung Rn. 337 f.
27 APD-Entscheidung Rn. 360.
28 APD-Entscheidung Rn. 346.
29 EuGH vom 5.06.2018, Rs. C-210/16 – Wirtschaftsakademie Rn. 39.
30 *EDSA*, Leitlinien 7/2020, Rn. 54.
31 APD-Entscheidung Rn. 370 f.

a. Einwilligung

Die Prüfung, ob eine Einwilligung nach Art. 6 I lit. a DSGVO als Rechtsgrundlage in Frage kommt, kommt zu einem schnellen Ende. Denn angesichts der Tatsache, dass der TC-String bislang nicht als personenbezogenes Datum behandelt wurde, wurde auch keine Einwilligung für dessen Verarbeitung eingeholt – vielmehr wurden die Nutzer:innen nicht einmal über die Verarbeitung informiert.[32]

b. Berechtigtes Interesse

Mögliche Rechtsgrundlage für eine Verarbeitung des TC-String bleibt also nur das berechtigte Interesse nach Art. 6 I lit. f DSGVO. Um sich auf berechtigtes Interesse berufen zu können, muss die Verarbeitung gemäß dem EuGH einer dreistufigen Prüfung standhalten:

1. Die:Der Verantwortliche muss mit der Verarbeitung einen legitimen Zweck verfolgen; 2. die Verarbeitung der personenbezogenen Daten muss für den legitimen Zweck erforderlich sein und 3. die grundlegenden Rechte und Freiheiten der betroffenen Person dürfen nicht verletzt werden (Abwägung).[33] Die ersten beiden Bedingungen sieht die Kammer als erfüllt an. Das Ziel der Verarbeitung des TC-Strings und der darin enthaltenen Nutzer:innen-Präferenzen, ist die Einhaltung von gesetzlichen Vorschriften und es werden auch nicht mehr Daten verarbeitet als notwendig. Schwerpunkt der Prüfung ist daher die dritte Bedingung. Hier müssen die Interessen der:des Verantwortlichen und die Rechte und Freiheiten der betroffenen Person gegenübergestellt werden. Mit Blick auf Erwägungsgrund 47 DSGVO ist dabei insbesondere zu beachten, ob die betroffene Person zur betreffenden Zeit im Kontext der Datenverarbeitung vernünftigerweise annehmen konnte, dass die Verarbeitung der Daten zu diesem Zweck stattfinden würde. Hierbei falle besonders ins Gewicht, dass die:der Nutzer:in weder über die Verarbeitung ihrer:seiner Daten in Form des TC-Strings, noch über den zur Speicherung des TC-Strings gesetzten Cookie, noch über Rechte in Hinblick auf die Verarbeitung, insbesondere das Widerspruchsrecht, aufgeklärt wird. Auch die große Zahl an Empfänger:innen wird von der Kammer betont. Die Abwägung führt dazu, dass die Kammer die dritte Bedingung als nicht erfüllt ansieht und im Ergebnis ein berechtigtes Interesse als Rechtsgrundlage ausschließt. Damit erfolgte die Verarbeitung von personenbezogenen Daten im TC-String ohne Rechtsgrundlage.[34]

4. Rechtsgrundlage für Verarbeitung von personenbezogenen Daten in RTB-Systemen

IAB Europe trifft nach den Ausführungen der Kammer auch für die nachgelagerte Verarbeitung von personenbezogenen Daten innerhalb von RTB-Systemen eine gemeinsame Verantwortung. Daher stellt sich auch hier die Frage, ob die Verarbeitung gemäß Artikel 6 I DSGVO rechtmäßig erfolgt. Als Rechtsgrundlagen kommen ebenfalls Einwilligung und berechtigtes Interesse in Frage.

a. Einwilligung

Das Einholen von Einwilligungen für die Verarbeitung von personenbezogenen Daten in RTB-Systemen ist Kernfunktion des TCF und letztlich einer der Zwecke, zu denen es entwickelt wurde. Dennoch stellt die Kammer erhebliche Mängel an einer freien und informierten Einwilligung fest.[35] Neben technischen Mängeln an dem vorgeschriebenen CMP-Interface und der nicht ausreichend klaren Beschreibung der Verarbeitungszwecke, kritisiert sie insbesondere zwei Aspekte:

Zum einen können Nutzer:innen unmöglich ausreichend informiert sein, da sie keine Möglichkeit haben, nachzuvollziehen, welche Daten die Ad-Tech-Vendoren und DMPs möglicherweise bereits über sie halten.[36]

Zum anderen merkt die Kammer an, dass die Zahl der möglichen Empfänger:innen der Daten so zahlreich ist, dass Nutzer:innen unverhältnis-

32 APD-Entscheidung Rn. 407.
33 EuGH vom 4.05.2017, Rs. C-13/16 – Rigas, Rn. 28-31.
34 APD-Entscheidung Rn. 413-425.
35 Zu den Anforderungen an ein solches: *EDSA*, Leitlinien 05/2020 V1.1.
36 APD-Entscheidung Rn. 437.

mäßig viel Zeit benötigen würden, um diese Information zu lesen – eine Einwilligung könne daher kaum informiert sein.[37]

Diese Feststellungen sind bemerkenswert, weil sie das Geschäftsmodell von RTB-Systemen treffen. Die Anzahl an Teilnehmenden zu reduzieren widerspricht dem Konzept, einen möglichst großen Adressat:innenkreis anzusprechen. Immerhin stellt das TCF ein Netzwerk dar, das gerade durch seine Größe und die daraus resultierende Kompatibilität mit vielen anderen Akteur:innen so interessant ist. Es ist auch fraglich, wie diesbezüglich eine Auswahl getroffen werden soll – aus wirtschaftlichen Gesichtspunkten wird die Entscheidung wohl auf die größten und lukrativsten Teilnehmenden fallen. Ein Ergebnis, das aus marktregulatorischen Gründen alles andere als wünschenswert erscheint und zu monopolartigen Strukturen führen könnte.

b. Berechtigtes Interesse

Ähnliche Erwägungen leiten die Bewertung, ob ein berechtigtes Interesse in Frage kommt. Wenig überraschend kommt die Kammer auch hier zu dem Schluss, dass ein berechtigtes Interesse keine Rechtsgrundlage für die Verarbeitungen im Rahmen des OpenRTB-Protokolls darstellt. Bereits das Erfordernis des legitimen Zweckes wird von der Kammer aufgrund von mangelnder Bestimmtheit als nicht erfüllt angesehen. Auch der Grundsatz der Datenminimierung werde nicht befolgt, sodass auch keine Erforderlichkeit vorliegt.

Bei der Interessenabwägung im dritten und letzten Prüfungsschritt wird die Kammer noch deutlicher: in Anlehnung an den EDSA komme berechtigtes Interesse bei Direktmarketing, das verhaltensorientierte Marketingstrategien nutzt, grundsätzlich nicht in Frage.[38]

c. Auswirkungen

Ein weiterer Satz sticht aus dem Volltext der Entscheidung heraus. Es ist ein Satz, dessen Inhalt den Ton der Entscheidung von Anfang an zu prägen scheint:
„The Litigation Chamber notes, for the record, that it is uncertain whether, in view of its current architecture and support of the OpenRTB protocol, the TCF can be reconciled with the GDPR".
In der Tat äußert die Kammer an einigen Stellen fundamentale Kritik an dem Modell des „Datenhandels" im Rahmen von RTB-Systemen, in denen Verhaltensprofile von Nutzer:innen an tausende von Empfänger:innen zum höchsten Preis versteigert werden.

Und es ist Kritik, die sich Betreibende dieser Systeme in den Augen von Datenschutzaktivisten gefallen lassen müssen. Nach Aussagen des Irish Council for Civil Liberties werden die Daten von US-Bürger:innen im Durchschnitt 747-mal am Tag durch RTB-Systeme offengelegt, die Daten von EU-Bürger:innen im Durchschnitt 376-mal am Tag. Das Online-Verhalten und der Standort von Nutzer:innen werde in den USA und Europa 178 Billionen mal im Jahr festgehalten.[39] Angesichts dieser Zahlen scheint es in der Tat schwer vorstellbar, dass Nutzer:innen der Umfang der Verarbeitung ihrer personenbezogenen Daten innerhalb der kurzen Zeit bewusst werden kann, die sie vernünftigerweise auf ein entsprechendes Pop-Up verwenden werden. Der Konflikt zwischen umfassender und gleichzeitig überschaubarer Information ist älter als die DSGVO selbst.[40] Offen bleibt also die Frage, ob es überhaupt möglich sein kann, die vom EDSA geforderten Mindestinformationen auf eine Art und Weise darzustellen, die durch Nutzer:innen in zumutbarer Weise aufgenommen und verstanden werden kann. Anzumerken sei aber auch, dass es fraglich bleibt, ob IAB Europe als Standardgeber wirklich der richtige Ansprechpartner für diese Form von Compliance ist – die Einordnung als Controller führt zu erheblichen Rechtsunsicherheiten und Risiken für die Herausgeber:innen von Standards,

37 APD-Entscheidung Rn. 435.

38 APD-Entscheidung Rn. 460; *Information Commissioner's Office*, Update report into adtech and real time bidding 20. Juni 2019 (1. Mai 2023).

39 *Irish Council for Civil Liberties*, RTB online ad auctions (1. Mai 2023).

40 *Menzel*, Datenschutzrechtliche Einwilligungen: Plädoyer für eine Rückkehr zur Selbstbestimmung, DuD 2008, 400 (408).

die demnach für eine unüberschaubare Anzahl an Verarbeitungsprozessen verantwortlich sein könnten, ohne davon zu wissen.

5. Berufungsentscheidung des Market Courts vom 07. September 2022

Dies ist jedoch eine Frage, die nicht mehr die APD beantworten wird, sondern der EuGH. Mit Beschluss vom 07. September 2022 wurden die Fragen nach der Qualifikation des TC-Strings als personenbezogenes Datum und der gemeinsamen Verantwortung von standardgebenden Organisationen durch das Berufungsgericht, den Market Court, als Vorlagefrage an den EuGH gestellt.[41]

IV. Real-Time-Bidding: Ein Auslaufmodell?

Während die Entscheidung des EuGH in Bezug auf das TCF noch abzuwarten ist, müssen sich AdTech-Anbieter:innen allgemein wohl auf veränderte Bedingungen einstellen.[42] Die Entscheidung des APD liest sich als klare Absage an ein Geschäftsmodell, das personenbezogene Daten zum Zwecke personalisierter Werbung an eine nahezu unüberschaubar große Menge an Empfänger:innen übermittelt. Auch die weiteren Datenschutzaufsichten der Mitgliedsländer, denen die Entscheidung durch die APD vorab übermittelt wurde, teilen diese Ansicht oder widersprechen ihr zumindest nicht.[43] Nun ist die Industrie gefragt, innovative Lösungen zu entwickeln, die AdTech mit bestehender und zukünftiger Regulatorik in Einklang bringen. Eine elegante Lösung wäre es sicherlich, Datenanonymität zu schaffen und somit gar nicht erst in den Anwendungsbereich der DSGVO zu fallen. Mit Blick auf die hohen Anforderungen an Anonymität ist dies sicherlich eine Herausforderung, zumal die Daten auch weiterhin sinnvoll nutzbar sein müssten. Es könnte einem Unternehmen aber auch einen entscheidenden Vorteil bringen – in einem Markt, der derzeit auf über 117 Milliarden $ geschätzt wird.[44]

41 *Hof van beroep Brussel vom 07.09.2022*, Market Court Document 2022/AR/292 – 2022/S7600, (1. Mai 2023).

42 So auch *Baumgartner/Hansch*, Onlinewerbung und Real-Time-Bidding, ZD 2020, 435 (439).

43 APD-Entscheidung Rn. 281.

44 *Irish Council for Civil Liberties*, RTB online ad auctions (1. Mai 2023).

• **Der Autor** studiert Rechtswissenschaft an der Universität Hamburg. Dieser Beitrag beruht auf einer im Seminar zum Datenschutzrecht bei Prof. Dr. Johannes Caspar eingereichten Seminararbeit.