EuGH: Datenschutz und Online-Werbung mit *Real Time Bidding*

» jusIT 2024/73

§ VO (EU) 2016/679: Art 4 Z 1 und Z 7, Art 26 Abs 1

EuGH 7. 3. 2024, C-604/22 (IAB Europe)

1. Eine Kombination aus Zahlen, Buchstaben und Zeichen, die die Einwilligung in die Verarbeitung personenbezogener Daten zur Online-Werbung enthält (hier: *Transparency and Consent String*), stellt ein personenbezogenes Datum iSv Art 4 Z 1 DSGVO dar, wenn sie einer Kennung wie der IP-Adresse zugeordnet werden kann.
2. Eine Branchenorganisation, die ihren Mitgliedern Regelungen zur Einwilligung und Verarbeitung personenbezogener Daten anbietet, kann als *„gemeinsam Verantwortlicher"* iSv Art 26 DSGVO gelten. Dies gilt insb, wenn sie Einfluss auf die Datenverarbeitung hat und die Zwecke sowie Mittel der Verarbeitung festlegt, auch wenn sie keinen direkten Zugang zu den Daten hat.
3. Die gemeinsame Verantwortlichkeit dieser Branchenorganisation erstreckt sich nicht automatisch auf die Weiterverarbeitung der Daten durch Dritte, wie Anbieter von Websites oder Apps, bezüglich der Nutzerpräferenzen für gezielte Online-Werbung.

Anmerkung des Bearbeiters:

Im aus Belgien stammenden Ausgangsfall entwickelte das *Interactive Advertising Bureau Europe* (*IAB Europe*), ein Verband der digitalen EU-Werbe- und Marketingwirtschaft, eine Technologie, die es in datenschutzrechtskonformer Weise ermöglichen sollte, Echtzeit-Auktionen um Werbeplätze (sog „*Real Time Bidding*") auf Internetseiten durchzuführen. Dabei können Werbeunternehmen, Datenbroker und Werbeplattformen, die Tausende von Werbetreibenden vertreten, anonym und in Echtzeit Gebote abgeben, um einen Werbeplatz auf einer Webseite zu erhalten und dort auf dem Profil des Nutzers, der gerade die Webseite aufruft, abgestimmte Werbung anzeigen (vgl instruktiv *Greiner*, Real-Time Bidding auf Websites – datenschutzfreie Zone?, ecolex 2020, 168). Die Belgische Datenschutzbehörde verhängte mangels Datenschutzkonformität gegen *IAB Europe* als verantwortliche Stelle mehrere Abhilfemaßnahmen sowie eine Geldbuße. Zusammengefasst stellte die Behörde Folgendes zum technischen Ablauf fest: Bevor eine nutzerspezifische Werbung angezeigt werden konnte, musste eine Einwilligung des Users zur Erhebung und Verarbeitung seiner personenbezogenen Daten für bestimmte Zwecke, wie Marketing, Werbung oder zum Austausch dieser Daten mit bestimmten Anbietern, eingeholt werden. Von besonderer Bedeutung waren dabei der Standort des Nutzers, sein Alter, der Verlauf seiner Suchanfragen und seiner zuletzt getätigten Einkäufe, wobei der Nutzer dem auch widersprechen konnte. Um das Einholen der Einwilligung technisch umzusetzen, wurden die Nutzerpräferenzen des sog „*Transparancy and Consent String*" (kurz: TC-String), der aus einer Kombination von Buchstaben und Zeichen besteht, kodiert und gespeichert (zur technischen Erläuterung siehe die Github-Page von *IAB* unter <bit.ly/DSB-TC> [17. 5. 2024]). Dieser würde dann mit anderen Datenverarbeitern geteilt, damit diese wissen, worin der Nutzer eingewilligt oder wogegen er widersprochen hatte. Auf dem Gerät des Nutzers würde zudem ein Cookie gespeichert. Miteinander kombiniert, können der TC-String und der Cookie der IP-Adresse dieses Nutzers zugeordnet werden. So erhält man nicht nur die notwendigen Informationen für ein effektives Cookie-Management-Tool, sondern auch zur Lead-Generierung (vgl *Thiele/Wagner*, B2B-Leads generieren und qualifizieren aus datenschutzrechtlicher Sicht, ZIIR 2023, 17 mwH).

IAB Europe legte daraufhin einen Maßnahmenplan vor, um die nach Auffassung der Behörde bestehenden Verstöße abzustellen. Dieser wurde auch Anfang des Jahres 2023 akzeptiert (abrufbar unter <bit.ly/DSB-APlan> [17. 5. 2024]). Dennoch erhob parallel dazu *IAB Europe* die Beschwerde an den Appellationshof Brüssel, der dem EuGH die Sache zur Vorabentscheidung vorlegte.

Die Vierte Kammer hielt fest, dass die von *IAB Europe* entwickelte Technologie in Form der TC-Strings zu personenbezogenen Daten iSv Art 4 Z 1 DSGVO führe, da sie ermögliche, in Kombination mit dem Cookie auf dem Gerät des Nutzers auch auf dessen IP-Adresse zuzugreifen. Auch wenn noch tatsächliche Fragen durch das vorlegende Gericht zu klären sind, nahm der EuGH bereits vorweg, dass *IAB Europe* bei der Speicherung der Einwilligungspräferenzen der Nutzer in einem TC-String auf die Verarbeitungen personenbezogener Daten Einfluss nahm und gemeinsam mit seinen Mitgliedern entschied, sowohl die Zwecke dieser Verarbeitungen als auch die ihnen zugrunde liegenden Mittel festzulegen. Allerdings müsste zur Bejahung der gemeinsamen Verantwortlichkeit iSv Art 26 DSGVO noch nachgewiesen werden, dass *IAB Europe* Einfluss auf die Festlegung der Zwecke und Modalitäten der Weiterverarbeitungen, die nach der Speicherung der Einwilligungspräferenzen der User in einem TC-String erfolgen, ausgeübt hatte.

Das vorliegende Urteil hat eine höchstrichterliche Klarstellung gebracht, die für die Online-Werbung im Grunde längst überfällig war: Dass auch eine mittelbare Identifizierbarkeit einer Person nur mit entsprechender Einwilligung rechtmäßig ist. Oberste Priorität im Kontext der Datenverarbeitung im Marketingbereich bleibt damit der Schutz der Nutzerdaten (vgl bereits EuGH 1. 10. 2019, C-673/17 [Planet49], jusIT 2019/90, 245; dazu *Dürager*, Der EuGH zur Zulässigkeit des Setzens von Cookies – eine endlose Geschichte ..., jusIT 2019/89, 241 mwH).

Bemerkenswert sind auch die Ausführungen zur gemeinschaftlichen Verantwortung. Diese erkennt der EuGH nämlich darin, dass *IAB Europe* berechtigt ist, von den Mitgliedern Informationen über die Identifizierbarkeit einzuholen (Rz 48 des Urteils). Die Vierte Kammer knüpft damit unmittelbar an ErwGr 26 zur DSGVO und die Vorjudikatur an (EuGH 10. 7. 2018, C-25/17 [Johovan Todistaja] Rz 66 ff, Dako 2019/9, 16 [*Haidinger/*

Weis] = jusIT 2018/59, 163 [*Thiele*] = ÖJZ 2018/114, 885 [*Lehofer*] = VbR 2018/110, 201 [*Leupold/Gelbmann*] = ZIIR 2018, 390 [*Thiele*]). Gleichwohl ergänzt das Urteil (in Rz 73 ff) zur Reichweite der gemeinsamen Verantwortung, dass sich diese nicht automatisch auf die Weiterverarbeitung der personenbezogenen Daten durch Dritte erstreckt, wie zB Website- oder App-Anbieter, insb in Bezug auf Nutzerpräferenzen für gezielte Online-Werbung.

Ausblick: Das vorliegende Urteil bietet durchaus Anlass, die in der Online-Branche eingesetzten *Real-Time-Bidding*-Verfahren zu evaluieren. Als Orientierung muss davon ausgegangen werden, dass eine Information (die Anbieter von Werbenetzwerken regelmäßig ohnehin als „*ID*" bezeichnen) ein personenbezogenes Datum darstellen kann, wenn dem jeweiligen Akteur eine Identifizierung unter Verwendung weiterer Daten möglich ist, auf die er Zugriff erlangen kann.

Zusammenfassend hat der EuGH entschieden, dass der sog „*Transparency and Consent String*" (TC-String), der ein wesentliches Element der Online-Werbung in Echtzeit darstellt, als personenbezogenes Datum iSv Art 4 Z 1 DSGVO einzuordnen sei, wodurch das Tool den Vorschriften der DSGVO unterfällt. Darüber hinaus sei der Verband, der den TC-String entwickelt hat, als Verantwortlicher iSv Art 4 Z 7 DSGVO anzusehen, wobei die bloße Berechtigung, von den Mitgliedern eines Branchenverbandes Informationen über die Identifizierbarkeit einzuholen, für eine gemeinschaftliche Verantwortlichkeit der Dachorganisation nach Art 26 DSGVO ausreicht.

Bearbeiter: Clemens Thiele

EuGH: Der nach innerstaatlichem Recht zu bemessende Schadenersatzanspruch gemäß Art 82 DSGVO setzt einen tatsächlichen (im)materiellen Schaden voraus

» jusIT 2024/74

§ VO (EU) 2016/679: Art 29, 82, 83

EuGH 11. 4. 2024, C-741/21 (juris)

1. Ein immaterieller Schaden iSv Art 82 Abs 1 DSGVO liegt nicht schon allein darin, dass gegen eine Bestimmung der DSGVO verstoßen wurde.
2. Der Verantwortliche wird nicht schon dadurch von seiner Haftung gem Art 82 Abs 3 DSGVO befreit, dass eine ihm unterstellte Person das schadensverursachende Fehlverhalten gesetzt hat.
3. Die Kriterien zur Bestimmung der Geldbußen nach Art 83 DSGVO eignen sich nicht für die Bemessung des Schadenersatzes nach Art 82 DSGVO, der iS des Grundsatzes der Verfahrensautonomie nach den innerstaatlichen Vorschriften zu ermitteln ist.
4. Die Anzahl der Verstöße, die ein Verantwortlicher gegenüber derselben betroffenen Person begangen hat, stellt kein relevantes Bemessungskriterium des Schadenersatzes dar.

Anmerkung des Bearbeiters:

Das Judikat entspringt einem Rechtsstreit zwischen einem Rechtsanwalt (Kläger) und *juris*, einer Gesellschaft, die in Deutschland eine juristische Datenbank betreibt (Beklagte). Nachdem der Kläger davon erfahren hatte, dass *juris* seine personenbezogenen Daten auch für Zwecke der Direktwerbung nutzte, widerrief er schriftlich alle seine Einwilligungen und widersprach jeglicher Verarbeitung seiner personenbezogenen Daten mit Ausnahme des Versands von Newslettern. Dessen ungeachtet erhielt der Kläger erneut Werbeschreiben, im Rahmen derer seine personenbezogenen Daten verarbeitet wurden. Seiner Ansicht nach sei ihm durch diese rechtswidrige Verarbeitung ein Schaden entstanden, weil er insb einen Verlust der Kontrolle über diese Daten erlitten habe. Deshalb erhob er Klage auf Schadenersatz. Die Beklagte wies jede Haftung zurück, weil sie einen Prozess zur Bearbeitung von Widersprüchen implementiert habe und die verspätete Berücksichtigung des Widerspruchs des Klägers auf ein weisungswidriges Verhalten eines ihrer Mitarbeiter zurückzuführen sei. Im Übrigen könne allein im Verstoß gegen eine Verpflichtung aus der DSGVO kein Schaden iSv Art 82 Abs 1 DSGVO liegen.

Den Vorlagefragen entsprechend behandelt das Judikat im Wesentlichen die Themen des immateriellen Schadenersatzes wegen Verlusts der Kontrolle über die eigenen personenbezogenen Daten, der Zurechnung von Fehlverhalten einer unterstellten Person sowie der Bemessungskriterien für die Höhe des Schadenersatzes insb bei gehäuften Verstößen gegen die DSGVO.

ErwGr 85 DSGVO nennt als Beispiel für einen aus der Verletzung des Schutzes personenbezogener Daten resultierenden Schaden den Verlust über deren Kontrolle. Wie der Gerichtshof klarstellt, muss dem Betroffenen wegen des Verstoßes gegen die DSGVO bzw *in concreto* des Verlusts über die Kontrolle jedoch tatsächlich auch ein (im)materieller Schaden entstanden sein (Rz 34 f).

Um sich von ihrer Haftung zu befreien, stützte sich die Beklagte auf Art 83 Abs 3 DSGVO, der das Verschuldenshaftungsregime (mit Beweislastumkehr) etabliert (EuGH 21. 12. 2023, C-667/21 [Krankenversicherung Nordrhein] Rz 93 f, Dako 2024/21, 44 [*Haidinger/Löffler*] = jusIT 2/2024, 60 [*Cepic*]). Das weisungswidrige Fehlverhalten einer iSv Art 29 DSGVO unterstellten Person könne der Beklagten als Verantwortlichem nicht zugerechnet werden. Mit Blick auf Art 32 Abs 4 DSGVO hält der Gerichtshof jedoch fest, dass der Verantwortliche neben den verpflichtenden Weisungen für unterstellte Personen iSv Art 29 DSGVO auch Maßnahmen zu treffen hat, dass diese Weisungen tatsächlich eingehalten werden (Rz 47 f). Da die Sicherheit der Verarbei-