46. Jahrgang
datenschutz-berater.de
DSB 02/2022

DATENSCHUTZ-BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

ISSN 0170-7256

dfv Mediengruppe

Heiko Markus Roth und Jannik Krone

Einstweilige Untersagung der Nutzung der Consent Management Plattform (CMP) „Cookiebot“

VG Wiesbaden, Urt. v. 1.12.2021 – 6 L 738/21.WI

Die Gerichtsentscheidung in Kürze

Innerhalb des vorläufigen Rechtsschutzes erwirkte der Nutzer einer Website erfolgreich eine einstweilige Anordnung gegenüber dessen Betreiber, es zu unterlassen, „Cookiebot“, einen bekannten CMP-Dienst, nicht zum Zwecke des Einholens von Einwilligungen einzubinden. Das Gericht begründete die voraussichtliche Rechtswidrigkeit im Wesentlichen mit einer nach Art. 44, 48 f. DSGVO unzulässigen Übermittlung in ein Drittland: Infolge der Einbindung erhalte auch die Muttergesellschaft des nachgelagerten CDN-Dienstleisters personenbezogene Daten, welche jedoch ihren Sitz in den USA habe und den Pflichten des CLOUD-Act unterliege.

Der Fall

Der Antragsgegner, die Hochschule Rhein-Main, hat auf ihrer Website Skripte für zwei Dienste eingebunden. Diese Skripte werden von den Servern des jeweiligen Anbieters geladen:

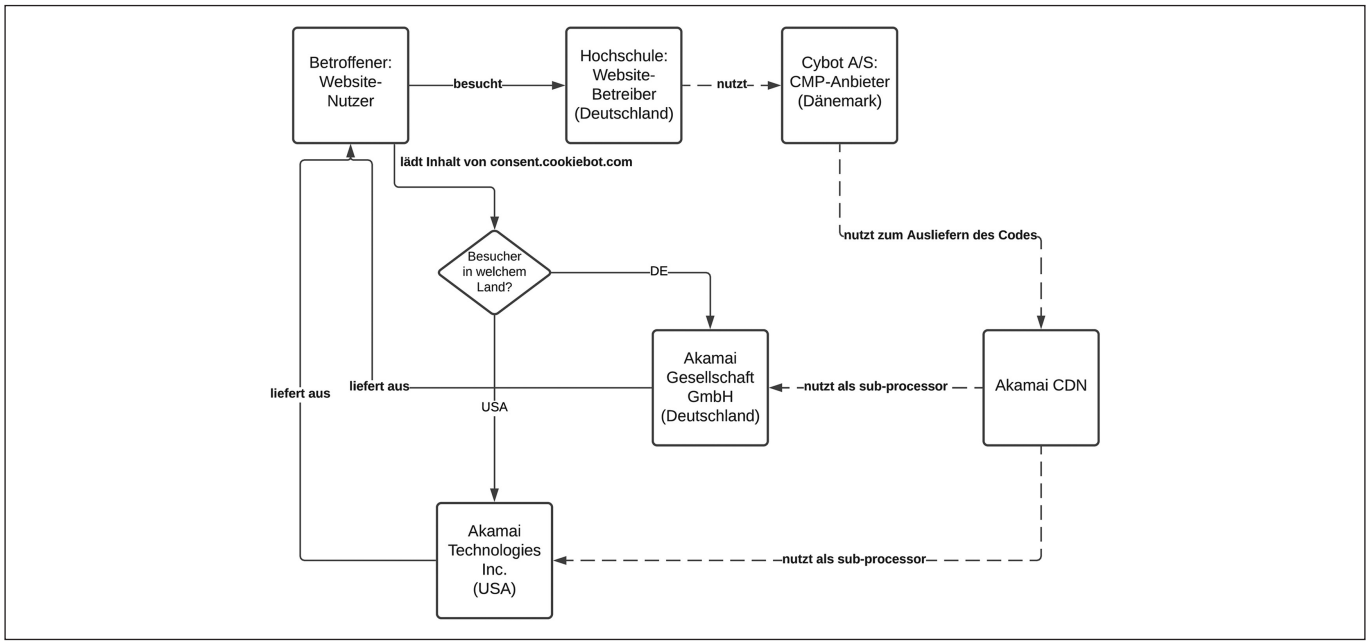
- „Cookiebot“ (Anbieter: Cybot A/S, Dänemark; Typ: integrierte Consent-Management-Platform, CMP) und
- “Google Tag Manager” (Anbieter: Google Ireland Ltd., Irland; Typ: Tag-Management-System, TMS, in dem der Code des CMP integriert ist).

Der Google Tag Manager wurde im Verfahrensverlauf ausgebaut und der Rechtsstreit diesbezüglich für erledigt erklärt; Cookiebot verblieb hingegen auf der Website.

Cookiebot ist ein Skript, dass eine „Cookie-Wall“ erzeugt, um das Setzen von Cookies von der vorherigen Einwilligung des Websitenutzers abhängig zu machen. Das Skript von Cookiebot wird von der Domain consent.cookiebot.com geladen. Die Domain löst zum Content-Delivery-Network (CDN) des Akamai-Konzerns auf, von dem auch das Skript geladen wird. Ein CDN stellt in der Regel global verteilte Serverkapazitäten für den Anbieter des CMP bereit, um ein schnelles Laden des Skriptes abhängig vom Standort des Websitenutzer durch Auswählen eines (geografisch) nahen Servers zu ermöglichen.

Interagiert der Nutzer mit dem CMP-Skript wird sowohl ein First-Party-Cookie gesetzt als auch ein Aufruf zu der obigen Domain getätigt. Als Cookie gespeichert und übermittelt werden sodann eine eindeutige ID zusammen mit den gewählten Einstellungen und einem Zeitstempel. Das CDN von Akamai löst unter gewissen Umständen zu IP-Adressen auf, die der Akamai Technologies Inc. mit Sitz in den USA oder der Akamai Technologies GmbH mit Sitz in Deutschland gehören.

Nachfolgend sind die einzelnen Entitäten und Datenflüsse auf Basis der aktuell verfügbaren Dokumente zum Datenschutz der CMP- und CDN-Anbieter visualisiert:



Der Antragsteller, ein Nutzer der Website, begehrte vom VG eine einstweilige Regelungsanordnung (§ 123 Abs. 1 Satz 2 VwGO) auf Unterlassung der Einbindung der CMP zum Zwecke des Einholens von Einwilligungen auf der Website (analog § 1004 BGB i. V. m. Art. 79 Abs. 1 und Art. 5 Abs. 1 lit. a DSGVO).

Die Gründe

Das VG bejaht im Ergebnis die Zulässigkeit und die Begründetheit des Rechtsbehelfs. Im Einzelnen:

Sperrwirkung von Art. 79 DSGVO?

Art. 79 DSGVO schließt den Rückgriff auf § 1004 BGB nicht aus. Ein Ausschluss würde im Widerspruch zum Recht auf „wirksamen" Rechtsbehelf nach Art. 79 DSGVO und zum europarechtlichen Effektivitätsgrundsatz stehen.

Hoheitliches Handeln?

Der Einsatz der CMP erfolgt im Rahmen der Öffentlichkeitsarbeit der Hochschule (§ 12 Abs. 5 Satz 4, Abs. 6 Satz 1 HHG). Insofern liege hoheitliches Handeln vor.

Eingriff in ein subjektiv-öffentliches Recht und Wiederholungsgefahr?

Durch die mit der CMP verbundenen Datenverarbeitung werde in das Recht des Antragstellers auf eine rechtmäßige Verarbeitung personenbezogener Daten, mithin ein subjektiv-öffentliches Recht, eingegriffen. Der Eingriff dauere auch an, da die CMP weiterhin auf der Website eingebunden ist.

Rechtswidrigkeit der Maßnahme?

Das VG prüft dann anhand der Art. 48, 49 DSGVO die Rechtswidrigkeit der Einbindung des CMP speziell mit Blick auf die Erhebung und die Übermittlung der IP-Adresse des Website-Nutzers sowie des für den Nutzer gesetzten Cookie-Keys. Thematisiert wurde im Einzelnen:

- Personenbezug der Daten: Nach Feststellung des VG verarbeiten jedenfalls Cybot A/S und Akamai die ungekürzte IP-Adresse des Nutzers der Website, jedenfalls durch Anlegen von Protokolldaten, die IP-Adresse und den Zugriffszeitpunkt enthalten. Das VG bejaht, ohne weitere Begründung und mit Verweis auf die Breyer Entscheidungen des EuGH (Urt. v. 19.10.2016 – C-582/14; Urt. v. 24.11.2011 – C-70/10) und des BGH (Urt. v. 16.05.2017 – VI ZR 135/13) den Personenbezug dieser IP-Adresse. Darüber hinaus finde eine Verarbeitung durch das Setzen eines Cookie-Keys („stamp") in Zusammenhang mit den weiteren verarbeiteten Daten statt. Für sich genommen ließe dieser Key noch keine Identifizierung einer bestimmten natürlichen Person zu. Der Key sei insofern „anonym", als er nicht mit dem Namen des Endnutzers in Verbindung gebracht werden könne. Erst im Zusammenspiel mit der ebenfalls übermittelten IP-Adresse und der übrigen Daten des Nutzers sei eine individuelle Zuordnung möglich. Im Ergebnis handele es sich daher auch bei dem Key um ein personenbeziehbares Datum.
- Verantwortlichkeit für die Verarbeitung: Unter Rückgriff auf die Grundsätze der phasenweisen Betrachtung des EuGH (Urt. v. 29.07.2019 – C-40/17; siehe dazu auch Lang, DSB 2019, 206 ff.) sei nach Ansicht des VG der Antragsgegner Verantwortlicher nach Art. 24, 4 Nr. 7 DSGVO für die Phase der Erhebung und der Übermittlung personenbezogener Daten (u. a. besagter IP-Adresse) an die Akamai-Gruppe, die unmittelbar durch die Einbindung des Dienstes auf der Website des Antragsgegners ausgelöst werden. Durch die Entscheidung für den Einsatz der konkreten CMP sowie in Kenntnis der Angaben des CMP- und des CDN-Anbieters entscheide der Antragsgegner über die Mittel und Zwecke der Datenverarbeitung. Das VG stellte explizit nicht auf eine gemeinsame Verantwortlichkeit ab, diese Zuordnung könne wegen Art. 26 Abs. 3 DSGVO vorliegend dahinstehen.
- Übermittlung in einen Drittstaat: Aufgrund des Sitzes der Unternehmenszentrale von Akamai (Akamai Technologies Inc.) in den USA komme es nach Ansicht des VG nicht darauf an, ob die Übertragung der Daten an die Server der Akamai Technologies Inc. oder der Akamai Technologies GmbH (Deutschland) erfolgt sei oder mit welchem der beiden Unternehmen der europäische CMP-Anbieter einen Vertrag habe. Aufgrund des CLOUD-Acts sei die Akamai Technologies Inc. zur Herausgabe aller Daten an US-Behörden verpflichtet, die sich in ihrem Besitz, Gewahrsam oder ihrer Kontrolle befinden. Eine solche Übermittlung an Behörden würde nicht von Art. 48 DSGVO gedeckt, da es an einer internationale Übereinkunft zwischen der USA und der EU fehle. Da auch keine der Voraussetzungen des Art. 49 Abs. 1 Satz 1 f. DSGVO vorliegen würden, sei die Übermittlung rechtswidrig. Art. 46 DSGVO erwähnt das VG nicht.

Kein Ausschlussgrund?

Die Rechtsverletzung des Antragstellers könne nur abgestellt werden, wenn die CMP insgesamt von der Website genommen werde. Ein nur partielles Abschalten der CMP ggü. dem Antragsteller sei technisch unmöglich.

Verbotene Vorwegnahme der Hauptsache?

Das Begehren des Antragstellers stellt auch keine verbotene Vorwegnahme der Hauptsache dar.

Auswirkungen auf die Praxis

Instanzgerichtliche Entscheidungen zu den Anforderungen an die Übermittlung in Drittstaaten sind, trotz der Entscheidung „Schrems II" des EuGH (Urt. v. 16.07.2020 – C-311/18; siehe dazu auch Pentzien/Lösch, DSB 2020, 222 ff.; Hansen-Oest, DSB 2020, 300 ff.), bisher rar. Der Bedarf solcher Entscheidungen ist ungebrochen, die relevanten Use Cases mit Drittland-Bezügen sind praktisch unzählig.

Neben bisherigen Entscheidungen aus Belgien, Luxemburg und Frankreich reiht sich nun auch das VG als erstes deutsches Gericht ein. Die Entscheidung war daher mit Spannung erwartet und wurde nach der Veröffentlichung vielerorts, sogar international, kommentiert. Bei all der Furore ist indes zu beachten: das VG prüft in dem vorliegenden Verfahren lediglich summarisch, ob der Antragsteller in der Hauptsache offensichtlich Erfolg haben wird bzw. bei schwierigen Rechts- oder Tatsachenfragen – wie in dem vorliegenden Fall – die Hauptsache lediglich nach dem ersten Anschein nicht unbegründet erscheint. Es wird sich zeigen, ob und wie die für die Hauptsache zuständige Kammer den Fall bewertet. Bei Analyse der Erwägungen des VG fallen im Einzelnen besonders nachfolgende Aspekte auf:

Keine Auseinandersetzung mit den SDK und den „zusätzlichen Maßnahmen" nach Schrems II

Das VG thematisiert weder das Instrument der Standarddatenschutzklauseln (SDK, Art. 46 Abs. 2 lit. c DSGVO; siehe dazu Grages, DSB 2020, 304 ff.), noch die vom EuGH in Schrems II geforderten „zusätzlichen Maßnahmen". Das überrascht nicht, legte die Hochschule wohl nur einen nicht ausgefüllten blanko „Standardvertragsklauseln (Auftragsverarbeiter)" zwischen Cybot und Akamai vor. Das Urteil enthält für die Praxis keine relevanten Ausführungen zu Standardvertragsklauseln, außer der Erkenntnis, dass man die Klauseln, auf die man sich berufen will, abschließen sollte. Mangels Vortrag oder Kenntnis setzt sich das Gericht auch nicht mit den zusätzlichen und auf der eigenen Website veröffentlichten Schutzmaßnahmen von Akamai auseinander.

Unzureichende Auseinandersetzung mit den einzelnen Verarbeitungs-Phasen

Das VG vollzieht die Verarbeitungsschritte beim CDN unzureichend nach. Lädt ein Websitebesucher aus Deutschland das CMP-Skript, wird die Domain zu Servern in Deutschland unter Kontrolle der Akamai Technologies GmbH aufgelöst und von diesen geladen. Zwar stehen die Domain und die DNS-Einträge unter der Kontrolle der Akamai Technologies Inc. Diese Gesellschaft verarbeitet aber bei der DNS-Auflösung keine Daten des Antragstellers. Vielmehr fragt der Browser des Nutzers beim DNS-Resolver seines Providers nach der korrekten IP-Adresse.

Die Verarbeitung verbleibt daher innerhalb der EU. Ein deutscher Nutzer ruft die Website einer deutschen Hochschule auf, dabei wird ein Skript eines dänischen Herstellers von einem deutschen Server geladen. Bei dieser Betrachtung erscheint unschlüssig, wieso das VG das Verbot der Verarbeitung überhaupt auf den Drittlandstransfer stützt, anstatt auf eine fehlende Vereinbarung zwischen der Hochschule und (letztlich) der Akamai Technologies GmbH. Das VG will es sogar „dahinstehen" lassen, ob konkreter Vertragspartner von Cybot das Unternehmen Akamai Technologies Inc. (Muttergesellschaft) oder die verbundene Akamai Technologies GmbH ist. Das VG lehnt folglich eine Betrachtung ab, wonach es auf den tatsächlichen Serverbetreiber oder den Verarbeitungsort ankommen könnte.

Überdehnung des Tatbestands der „Übermittlung"

Stattdessen lässt es das VG für das Vorliegen einer „Übermittlung" ausreichen, dass die Unternehmenszentrale des CDN-Anbieters in den USA ihren Sitz habe und diese daher dem Anwendungsbereich des CLOUD-Act (Title 18 U. S. C. § 2713) unterliege.

Weder betrachtet das VG, ob die deutsche Gesellschaft eigenständige Entscheidungen über die Offenlegung treffen kann, noch ob eine solcher Vorgang in die USA überhaupt erfolgt. Diese Interpretation birgt auch politische Sprengkraft: bietet eine Organisation mit Sitz in Deutschland datenverarbeitende Dienstleistungen an und gehört diese Organisation zu einem Konzern, dessen Muttergesellschaft ihren Sitz in den USA hat und dem CLOUD-Act unterliegt, wird dieses verbundene Unternehmen faktisch unter den Generalverdacht des Rechtsbruchs bzw. der Spionage für US-Behörden gestellt.

Das VG interpretiert „Übermittlung" also nicht als faktischen Vorgang im Sinne einer Übertragung elektronischer Signale oder gar einer tatsächlichen Zugriffsmöglichkeit. Das VG setzt vielmehr das hypothetische Risiko eines zukünftigen Datenzugriffs, gestützt auf den CLOUD-Act, einer „Übermittlung" gleich. Diese Interpretation findet jedoch keinen Halt in der DSGVO, weder im Wortlaut noch in der Systematik des Art. 44 DSGVO.

Im Gegenteil: Die Akamai Technologies GmbH unterliegt selbst der DSGVO und darf nach – auch vom VG selbst zitierten – Art. 48 DSGVO gar keine Daten an US-Behörden weitergeben. Verschaffen sich US-Behörden dennoch unberechtigt Zugriff zu den Daten der GmbH, liegt vielmehr ein Verstoß gegen Art. 32 Abs. 1 lit. c DSGVO vor.

Die Ansicht des Gerichts ist insbesondere deshalb irritierend, da die Konzern-SDK von Akamai ausdrücklich den Datenexport der IP-Adresse als Teil von Log-Dateien an Akamai Technologies Inc. in den USA und auch zusätzliche Maßnahmen vorsehen. Mit dieser nachprüfbaren Sachlage setzt sich das Gericht nicht auseinander, sondern springt direkt zu einem Verbot des Datentransfers, da sich die Unternehmenszentrale in den USA befände.

Es bleibt zu hoffen, dass diese Interpretation auf keinen weiteren Nährboden in der Rechtsprechung stößt, insbesondere mit Blick auf die Pflichten der EU aus internationalen Handelsabkommen.

Handlungsanweisung für die Praxis/Fazit

Spätestens seit „Schrems II“ ist die Verarbeitung in Drittstaaten in den Fokus der Öffentlichkeit gelangt. Auch Aufsichtsbehörden reagieren zusehends. Während hierzulande zuletzt eine länderübergreifende Prüfaktion zum internationalen Datenverkehr anhand diverser Dienste gestartet wurde (z. B. Einsatz von Webhostern), gab es etwa in Portugal bereits eine Nutzungsuntersagungen im Zusammenhang mit der Beauftragung eines US-CDN.

Der Fall zeigt, dass es gar nicht zum Einschreiten durch die Aufsichtsbehörde kommen muss, sondern auch Dritte (z. B. Datenschutzaktivisten) auf die Einhaltung klagen können. Webseitenbetreiber, die Inhalte von Dritten in Drittstaaten einbinden oder Dienste Dritter in Anspruch nehmen, die „in der Kette“ durch Sub-Beauftragungen Übermittlungen in Drittstaaten auslösen, müssen vorweg sicherstellen, dass diese Integration den Anforderungen der Art. 44 ff. DSGVO entspricht.

Dabei ist (spätestens) mit dem Inkrafttreten der neuen SDK unabdingbar, die Rollen aller an der Verarbeitung Beteiligten korrekt zu ermitteln. Vorliegend hätte die Hochschule entweder mit Akamai selbst die SDK-Klauseln nach Modul zwei (C2P) abschließen müssen oder, sofern dies aufgrund der Verarbeitung zulässig wäre, mit Cybot einen Auftragsverarbeitungsvertrag (AVV) und Cybot mit Akamai die SDK-Klauseln nach Modul drei (P2P). Akamai selbst bietet den Kunden sowohl an, den P2P-SDK beizutreten als auch den Abschluss der C2P-SDK.

Sich darauf zu berufen, dass Daten nicht direkt aus dem eigenen Verantwortungsbereich, sondern erst von einem anderen Verantwortlichen in einen Drittstaat übermittelt werden und diese Trennung einen selbst „freizeichnet“, ist, wie in diesem Fall, zum Scheitern verurteilt. Schließlich ist noch zu konstatieren, dass der entschiedene Fall aufgrund seiner atypischen Gestaltung (u. a. kein AVV zwischen Websitebetreiber/CMP-Anbieter, keine SDK) und den summarischen Prüfsätzen – leider – nicht geeignet ist, generelle Leitsätze zu entwickeln. Viele wichtige Fragen im Kontext des Kapitel V DSGVO bleiben damit offen.

Autoren: **Heiko Roth, LL. M., ist interner DSB im Konzernumfeld.**

Jannik Krone ist Syndikusrechtsanwalt und Rechtsanwalt und schwerpunktmäßig im Datenschutz und IT-Recht tätig.

Der Beitrag spiegelt die private Meinung der Autoren wider.