



Informationsblatt zur Entscheidung der belgischen Datenschutzaufsicht zu Cookie-Bannern des IAB Europe

Inhaltsverzeichnis

1. Was hat die belgische Datenschutzaufsicht entschieden?	1
2. Warum ist die Entscheidung der APD auch in Deutschland relevant?	3
3. Ist Ihr Unternehmen von dieser Entscheidung betroffen?	3
4. Was Sie jetzt tun sollten.....	3

1. Was hat die belgische Datenschutzaufsicht entschieden?

Am 2. Februar 2022 hat die belgische Datenschutzaufsichtsbehörde APD (Autorité de protection des données) eine Entscheidung¹ veröffentlicht, welche den europaweit verbreiteten Standard des sogenannten „Transparency and Consent Framework“ (TCF) zum Einwilligungsmanagement für Cookies und Tracking auf Webseiten und in Apps betrifft.

Dieser Standard wurde von dem IAB Europe (Interactive Advertising Bureau) entwickelt und wird derzeit auf fast 80 % der Webseiten und Apps in Europa genutzt. Der IAB Europe ist der europäische Verband für digitales Marketing und Werbung mit einer Vielzahl von Mitgliedern. Dessen Open-Source-Standard bot bisher Webseitenbetreibern und App-Anbietern die Möglichkeit, die Zustimmung der Nutzer zur Schaltung gezielter Werbung einzuholen. Nicht nur ist dieses System bei beinahe allen Online-Medien implementiert, auch große Digitalkonzerne wie etwa Google oder Amazon verwenden diesen Standard.

Nach Ansicht der belgischen Datenschutzbehörde verstößt dieser gegen die Europäische Datenschutzgrundverordnung (DSGVO). Die über dieses Einwilligungsmanagement-System generierten TC-Strings² stellen personenbezogene Daten dar, die zusammen mit dem gesetzten TCF-Cookie und der IP-Adresse eines Webseitenbesuchers oder App-Nutzers die jeweilige Person eindeutig identifizierbar machen. Im Ergebnis sei nach Auffassung der APD davon auszugehen, dass

¹ Englische Übersetzung der Entscheidung abrufbar von der Webseite der belgischen Datenschutzaufsicht hier: <https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf>

² Der IAB TC String ist eine codierte Zeichenkette, die alle relevanten Informationen rund um den Consent des Nutzers enthält und an sämtliche Parteien weiterreicht.



Webseitenbesucher und App-Nutzer, die ihre Einwilligung über ein Cookie-Banner auf der Grundlage des TCF-Standards abgegeben haben, nicht hinreichend transparent und verständlich über die Verarbeitung ihrer Daten informiert wurden. Das Einwilligungsmanagement schütze die personenbezogenen Daten der Nutzer nicht und ermögliche es ihnen nicht, ihre Rechte effektiv auszuüben.

Grundsätzlich sei davon auszugehen, dass den Betroffenen bei diesen Cookie-Bannern nicht klar sei, dass Aufzeichnungen über die Einwilligung geführt werden. Darüber hinaus seien einige der angegebenen Verarbeitungszwecke zu allgemein formuliert, als dass diese die betroffenen Personen angemessen über den genauen Umfang und die Art der Verarbeitung ihrer personenbezogenen Daten informieren würden. Ein differenziertes Verständnis all der unterschiedlichen Verarbeitungszwecke und Empfänger (eine oder mehrere Werbe-Anbieter) sei nicht möglich. Häufig sei den Webseitenbesuchern oder App-Nutzern nicht die Vielzahl der Datenempfänger klar, was ein Verstoß gegen das Transparenzgebot der DSGVO sei. Insgesamt wurden von der APD Verstöße gegen DSGVO Anforderungen der Rechtmäßigkeit und Transparenz (Artt. 5 Abs. 1, 6, 12, 13 und 14 DSGVO) sowie der Sicherheit der Verarbeitung, Unversehrtheit der personenbez. Daten, Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Artt. 24, 25, 5 Abs. 1 f und 32 DSGVO) festgestellt.

Die Folge der Entscheidung der belgischen Datenschutzaufsichtsbehörde ist, dass fortan Cookie-Banner Systeme, die auf dem TCF Standard basieren, als unwirksam gelten und somit keine gültige Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten der Webseitenbesucher bzw. App-Nutzer besteht. Andere Rechtsgrundlagen, wie etwa Vertrag (Art. 6 Abs. 1 b DSGVO) oder das berechnete Interesse (Art. 6 Abs. 1 f DSGVO) sind nicht geeignet, die Datenverarbeitung hinreichend zu legitimieren.

Nach Auffassung der APD hat ferner IAB Europe – obgleich dazu verpflichtet – kein Verzeichnis der Verarbeitungstätigkeiten geführt (Artikel 30 DSGVO), keine Datenschutzfolgenabschätzung durchgeführt (Art. 35 DSGVO) sowie keinen Datenschutzbeauftragten bestellt (Art. 37 DSGVO). In dem Zusammenhang hat die APD festgestellt, dass **IAB Europe gemeinsam mit allen beteiligten Organisationen (wie etwa die Webseitenbetreiber) mit verantwortlich für die Datenverarbeitung** sei. Eine Mithaftung der IAB für die Verstöße sei gegeben.

Darüber hinaus sei offensichtlich, dass etliche TCF-basierte Einwilligungsmanagement-Lösungen die erfassten personenbezogenen Daten außerhalb des Europäischen Wirtschaftsraums (EWR) an eine Vielzahl von Werbe-Anbietern übermitteln. **Somit eröffnet sich das zusätzliche Problemfeld der im Sinne der Artt. 44-49 DSGVO nicht hinreichend legitimer Drittstaatenübermittlungen.** Webseitenbetreiber und App-Anbieter seien hierbei gemeinsam mit IAB Europe verantwortlich und rechenschaftspflichtig, die notwendigen Maßnahmen zu ergreifen, um zu verhindern, dass personenbezogene Daten, die über ihre Website und/oder Anwendung erhoben wurden, ohne angemessene internationale Übermittlungsmechanismen außerhalb des EWR übermittelt werden.



2. Warum ist die Entscheidung der APD auch in Deutschland relevant?

Die Entscheidung der belgischen Datenschutzaufsichtsbehörde wurde in einem sogenannten „One-Stop-Shop“-Verfahren gefällt. Dies bedeutet, dass bei grenzüberschreitender Datenverarbeitung die für den Verantwortlichen (hier: IAB Europe) zuständige Datenschutzaufsichtsbehörde federführend ist. Die Entscheidung dieser Aufsichtsbehörde gilt dann jedoch europaweit.

3. Ist Ihr Unternehmen von dieser Entscheidung betroffen?

Wenn Ihr Unternehmen ein Webseitenbetreiber oder App-Anbieter ist, der das Transparency & Consent Framework (TCF) des IAB Europe nutzt oder wenn Sie auf Ihrer Webseite Werbung auf Grundlage des ebenfalls von IAB Europe entwickelten OpenRTB Protokolls anzeigen lassen, sind Sie von der Entscheidung betroffen.

Das OpenRTB Protokoll wird zum Beispiel auch in bestimmten Fällen von Google AdSense integriert. Wenn Sie ein Tool zum Einwilligungsmanagement bzw. zur Einbindung von Cookie-Bannern nutzen, (z. B. von Usercentrics, Borlabs Cookie, CookieBot, OneTrust oder Cookieinformation), sollten Sie umgehend prüfen, inwieweit deren eingebundene Lösungen den TCF Standard verwenden. Ist dies der Fall, sind Sie ebenfalls von der Entscheidung betroffen.

Dann müssen Sie davon ausgehen, dass über Ihr Cookie-Banner auf Ihrer Webseite oder in Ihrer App derzeit potenziell keine wirksamen Einwilligungen eingeholt werden. Es ist möglich, dass Sie von zuständigen Datenschutzaufsichtsbehörden dazu aufgefordert werden, das Setzen von Cookies, Datenerhebung von Webseitenbesuchern/App-Nutzern und die Schaltung von Werbung umgehend einzustellen. Ferner ist es möglich, dass Sie von der Datenschutzaufsichtsbehörde bei Nichtbefolgung mit Bußgeldern belegt werden.

Nur dann, wenn Ihr Unternehmen lediglich auf Webseiten oder Apps anderer Organisationen ihre Werbung schalten lässt, sind Sie nicht unmittelbar von der Entscheidung betroffen.

4. Was Sie jetzt tun sollten

Betroffene Unternehmen sollten nun im Hinblick auf die Entscheidung der belgischen Datenschutzaufsicht eine Reihe von Maßnahmen in Angriff nehmen, um ihr Bußgeldrisiko zu mindern. Diese sind:

1. Überprüfung der eigenen Firmenwebseiten hinsichtlich der Nutzung von Cookie-Bannern wie auch Cookies und anderen Trackingwerkzeugen. Hierbei ist festzustellen, was für ein Cookie-Banner genau eingebunden ist und ob dieses auf dem Transparency & Consent Framework (TCF) des IAB Europe basiert.
2. Beruht das auf Ihrer Webseite eingebundene Consent Banner auf dem TCF-Standard, so sollten Sie sich umgehend mit dem Anbieter für dieses Einwilligungsmanagement-Tool in Verbindung setzen, um eine ordnungsgemäße und DSGVO-konforme Lösung zu erreichen. Ist dies nicht möglich, können Sie auch auf einen anderen Anbieter umschwenken, der DSGVO-konforme Einstellmöglichkeiten in seinem Consent-Banner-Produkt anbietet und zudem



keine Subunternehmer mit Sitz in einem Drittstaat im Einsatz hat, wie z. B. [Consentmanager](#), [CCM19](#) (nur als On-Premise-Lösung). Achten Sie bei der Implementierung darauf, die Anforderungen der DSGVO, dem TTDSG und der Datenschutzaufsichtsbehörden entsprechend umzusetzen. Detaillierte Informationen zu den Anforderungen können Sie unserer kurzen Hilfestellung entnehmen, die wir Ihnen mit unserem Newsletter zu dem Thema beigefügt haben.

3. Darüber hinaus sollten Sie eine generelle Bestandsaufnahme durchführen, für welche Zwecke die eingesetzten Cookies und Tracking-Werkzeuge jeweils genutzt werden und ob eine Einwilligung der Webseitenbesucher erforderlich ist. Erfahrungsgemäß werden hier häufig Dinge übersehen, so dass mehr Daten erhoben werden als beabsichtigt. Erforderlichenfalls sollte eine entsprechende Anpassung der Datenschutzerklärung und des Consent-Banners der Webseite/App erfolgen. Hierbei sollte beachtet werden, dass bei allen Daten, die in irgendeiner Weise zu Marketingzwecken genutzt werden, die Einwilligung des Webseitenbesuchers oder App-Nutzers einzuholen ist.

Die belgische Datenschutzaufsicht hat der IAB Europe erlaubt, innerhalb einer Frist von sechs Monaten zu versuchen, das TCF-Einwilligungssystem anzupassen, damit dieses DSGVO konform wird. Gelingt dies der IAB Europe nicht, ist mit Zwangsgeldern und weiteren Bußgeldern zu rechnen. Die IAB Europe hat bereits Stellung genommen und angekündigt, gegen die Entscheidung der APD rechtlich vorgehen zu wollen. Hierbei wurde allerdings auch angekündigt, dass der TCF-Standard angepasst werde.

Da alle diesen Standard nutzenden Unternehmen datenschutzrechtlich mitverantwortlich sind, sind diese nun davon abhängig, dass es der IAB Europe gelingt, die zuständige Datenschutzaufsicht oder notfalls die Gerichte in einem Verfahren gegen die Entscheidung der APD zufrieden zu stellen. Der Ausgang ist hier ungewiss. Hier wird die IAB Europe lediglich mit einer deutlich verbesserten Ausgestaltung der Consent-Banner mit transparenterer Information vor Einwilligungsabgabe punkten können.

Bezüglich der anderen Datenschutzaufsichtsbehörden in Europa wird abzuwarten sein, wie diese sich verhalten. Es ist möglich, dass diese zunächst die sechs Monate abwarten, um zu sehen welche Veränderungen die IAB Europe vornimmt. Es verbleibt dennoch für betroffene Webseitenbetreiber und App-Anbieter ein Restrisiko im Hinblick auf Prüfungen und ggf. Sanktionen durch die für sie zuständigen Datenschutzaufsichtsbehörden.

Kontaktieren Sie uns, wenn wir Sie Fragen haben oder Beratung bei der Umsetzung unserer oben genannten Handlungsempfehlungen benötigen. Wir helfen Ihnen gerne und mit Sachverstand weiter.

Ihr Floß Team

Stand des Dokuments: 07.06.2022