Ausgabe 02/2022

Liebe Leserin, lieber Leser,

in unserem neuen Newsletter liegt der Fokus auf verschiedenen Urteilen und Entscheidungen, die wir für Sie detailliert aufbereitet haben. In Bezug auf das Urteil zu Google Fonts zeigen wir Ihnen die Möglichkeit auf, dies weiterhin datenschutzkonform einzubinden. Auch gehen wir auf eine Entscheidung der belgischen Datenschutzbehörde zum Real-Time-Advertising ein, welche für die gesamte EU gilt.

Unsere Themen und Quellen im Überblick:

- **LG München I: 100 € Schadensersatz für den Einsatz von Google Webfonts**
  https://www.datenschutz-guru.de/lg-munchen-i-100-schadensersatz-fur-den-einsatz-von-google-webfonts/

- **250 TEUR Bußgeld gegen IAB Europe - Verbot von Real-Time-Advertising?**
  https://www.linkedin.com/pulse/250k-bu%25C3%259Fgeld-gegen-iab-europe-verbot-von-dr-thomas-schwenke/

- **Französische Datenschutzbehörde CNIL hält Google Analytics für unvereinbar mit der DSGVO**
  https://www.datenschutzticker.de/2022/02/franzoesische-datenschutzbehoerde-cnil-haelt-google-analytics-fuer-unvereinbar-mit-der-dsgvo/

- **Urteile**

- **weitere interessante Links**

Viel Spaß beim Lesen,

freundliche Grüße

Mario Barthel

➢ LG München I: 100 € Schadensersatz für den Einsatz von Google Webfonts

In unserem letzten Newsletter haben wir Sie bereits auf das Urteil bezüglich Google Fonts (früher: Google Webfonts) hingewiesen. Hierbei erhielt ein Besucher einer Webseite 100 € Schadensersatz, da der Betreiber der Webseite Google Fonts per Link eingebunden hatte.

Dies ist sicherlich kein großer Betrag, kann sich aber deutlich erhöhen, wenn nicht nur ein Besucher klagt, sondern im Rahmen einer Massenklage vorgegangen wird. Für ein besseres Verständnis möchten wir Sie darüber informieren, was Google Fonts sind und wie man sie mit einer einfachen Lösung datenschutzkonform einbinden kann.

Was sind Google Fonts?

Mit dem Dienst Google Fonts ermöglicht es Google LLC Webseitenbetreibern kostenfrei, ca. 1.300 Schriftarten auf der eigenen Webseite einzubinden. Dies bietet den Vorteil, dass Besuchern der Webseite immer ein einheitliches Erscheinungsbild geboten wird, auch wenn sie die Schriftart nicht auf ihrem Endgerät installiert haben. Problematisch ist jedoch, dass beim Besuch der Webseite die Schriftarten nachgeladen werden. In dem Moment besteht eine Serververbindung zu Google LLC in den USA und die IP-Adresse des Webseitenbesuchers wird für die Auslieferung der Schrift an Google übertragen.

Wie kann ich Google Fonts datenschutzkonform einbinden?

Die Antwort lautet: Mit einer lokalen Einbindung der benötigten Schriftarten. In diesem Fall findet keine Verbindung zum Server von Google LLC in den USA statt.

Dies ist möglich, da Google es erlaubt, die „Google Fonts“ herunterzuladen und auf dem eigenen Server zu speichern und zu verwenden. Diese Seite kann dabei helfen: https://google-webfonts-helper.herokuapp.com/fonts.

Um ein mögliches Risiko in Bezug auf Datentransfer auszuschließen, bietet sich folgendes Vorgehen an:

1. **Prüfen Sie Ihre Webseite auf mögliche Verbindungen zu Drittanbietern** (z.B. mit dem „Netzwerkanalyse“-Tool der Webdeveloper-Tools des Browsers). Aufrufe, die „fonts.googleapis.com“ oder „fonts.gstatic.com“ beinhalten, weisen darauf hin, dass Server von Google aufgerufen werden. Diese „Fonts“-Server befinden sich mit großer Wahrscheinlichkeit aktuell in den USA.

2. **Identifizieren Sie die Schriftarten und Schrifttypen**, die auf der Webseite verwendet werden. Wenn möglich sollte die Anzahl der Schriftarten möglichst gering sein, um die Ladezeiten zu verkürzen (wichtig beim Suchmaschinenranking).

3. **Binden Sie die gewählten Schriftarten lokal ein**.

4. **Testen Sie die Ladezeit der Webseite (z. B. mit GTmetrix)**.

➢ 250 TEUR Bußgeld gegen IAB Europe - Verbot von Real-Time-Advertising?

Die belgische Datenschutzbehörde (APD) hat das Einwilligungsverfahren auf Grundlage des „Transparency & Consent Framework (TCF)“ von IAB Europe, einen für die Onlinewerbung zentralen Standard, für datenschutzrechtlich unzulässig und damit praktisch das Real-Time-Advertising für unwirksam erklärt. Gegen die Werbe-Organisation IAB Europe wurde ein Bußgeld von 250.000 Euro verhängt. Die Entscheidung ist nach dem "One Stop Shop"-Prinzip der Datenschutz-Grundverordnung gefallen und gilt somit für die gesamte EU.

Das Transparency & Consent Framework (TCF) ist der zentrale Standard hinter Cookie-Bannern und personalisierter Werbung und somit Grundlage für das sog. Real-Time-Advertising/Bidding (welches wiederum auf dem OpenRTB-Protocol basiert). Betritt ein Nutzer eine Webseite, findet in Echtzeit ein Bieterwettbewerb von sog. "Advertisern", also Werbung schaltenden Unternehmen, um die Werbeanzeigeplätze auf dieser Webseite statt. Klickt ein Nutzer bei einem Cookie-Banner auf „Akzeptieren“ wird ein TC-String erzeugt und an alle Partner geschickt, die an dem Bieterwettbewerb teilnehmen. Aufgrund dieses TC-Strings werden Nutzerprofile zusammengestellt, die dann die Grundlage für Echtzeit-Werbeauktionen bilden, mit denen einzelne Werbeplätze unter oft Hunderten Firmen versteigert werden.

Die belgische Datenschutzbehörde hat jetzt festgestellt, dass der TC-String eine personenbezogene Nutzer-Identifikationsnummer ist und nach den Vorgaben der DSGVO behandelt werden muss. Hieraus ergibt sich Weiteres:

- Die Verarbeitung des TC-String ist **unzulässig** und die eingeholten **Einwilligungen sind unwirksam**. Die Nutzer wissen nicht, in was sie einwilligen, weil die Verarbeitungsverfahren zu **i**ntransparent sind. Die Nutzer wissen gar nicht, dass deren Daten live im Internet gehandelt werden.
- Aufgrund der Intransparenz scheiden auch **berechtigte Interessen** als Erlaubnisgrundlage aus.
- Ferner ist nach Ansicht der Behörde, IAB Europe für die Verarbeitung dieser Nutzeridentifikationsnummer **gemeinsam mit den Publishern verantwortlich.**
- Als Verantwortliche hat die IAB Europe ihre Pflichten, u.a. zur Ergreifung der nötigen **Sicherheits- und Kontrollmaßnahmen**, Führung eines **Verarbeitungsverzeichnisses**, **Datenschutz-Folgenabschätzung, Vereinbarung über gemeinsame Verantwortlichkeit** und Benennung eines **Datenschutzbeauftragten** nicht wahrgenommen

Die IAB Europe will rechtlich gegen diese Entscheidung vorgehen.

Wenn Sie das Transparency & Consent Framework (TFC) nutzen oder auf Ihrer Webseite Werbung auf Grundlage des OpenRTB-Protokolls anzeigen lassen (z.B. Google Adsense, s. in welchen Fällen) ist davon auszugehen, dass Sie potenziell **keine wirksamen Einwilligungen** nutzen. Aufsichtsbehörden könnten Sie zur Einstellung von Werbeschaltungen auf Grundlage von TCF/OpenRTB auffordern, sowie bei Nichtbefolgung Bußgelder verhängen.

➢ Französische Datenschutzbehörde CNIL hält Google Analytics für unvereinbar mit der DSGVO

In unserem letzten Newsletter haben wir Sie über die Entscheidung der österreichischen Datenschutzbehörde (DSB) informiert, dass die Übermittlung personenbezogener Daten in die USA aufgrund der Nutzung des Trackingtools „Google Analytics“ auf einer österreichischen Webseite nicht als datenschutzkonform einzustufen ist und somit einen Datenschutzverstoß darstellt.

Jetzt hat auch die französische Datenschutzbehörde CNIL in ihrer Stellungnahme vom 10. Februar 2022 dazu aufgefordert, dass Webseiten mit europäischen Besuchern auf den Einsatz von Google Analytics verzichten sollen. Laut CNIL reichen auch die von Google getroffenen zusätzlichen Schutzmaßnahmen nicht aus, um den Zugriff durch US-Geheimdienste auszuschließen.

Hintergrund für die Entscheidung sind auch hier Beschwerden der von Max Schrems gegründeten Organisation NOYB. NOYB hat bei fast allen Datenschutzbehörden der EU-Staaten Beschwerden vorgebracht, so dass weitere Entscheidungen zu erwarten sind. Google fordert unterdessen dringend einen Privacy-Shield-Nachfolger.

➢ Urteile

<u>Werbung in Double-Opt-In-Bestätigungsmail unzulässig</u>

In dem Fall ging es um Zusendung von unzulässiger Werbung in Form einer Newsletter-Bestätigungsmail im Double-Opt-In Verfahren. Die Bestätigungsmail enthielt neben dem Bestätigungslink das Logo sowie den Satz „Welcome to ZzZzZzZzZ “ und „Hast du Fragen zum Newsletter? Kontaktiere uns über: info@ZzZzZzZzZ.de“. Der Kläger machte daraufhin Schadensersatz geltend.

Das Gericht sah es hier als gegeben an, dass die Bestätigungsmail über eine reine Aufforderung zur Bestätigung hinausging und werbende Inhalte enthielt. Im Gegensatz dazu sei eine bloße Absenderangabe grundsätzlich zulässig. Dem Kläger wurde Schadensersatz in Höhe von 179,27 € zugesprochen.

Urteil des LG Stendal vom 12. Mai 2021 - Az.: 22 S 87/20

<u>Der Geschäftsführer einer GmbH ist neben der Gesellschaft „Verantwortlicher“ im Sinne der DSVGO</u>

In diesem Fall wurde der Kläger durch einen vom GmbH-Geschäftsführer beauftragten Detektiv ausgespäht. Der Detektiv sollte recherchieren, ob der Kläger in der Vergangenheit an möglichen strafrechtlich relevanten Handlungen beteiligt gewesen war. Jedoch fehlte es bei dieser veranlassten Datenverarbeitung laut des OLG Dresden an der Erforderlichkeit zur Wahrung der berechtigten Interessen der Beklagten im Sinne von Art. 6 Abs. 1 lit. f DSGVO, so dass dies einen Datenschutzverstoß darstellt.

Das Gericht stufte den Geschäftsführer neben der GmbH als eigenen datenschutzrechtlich Verantwortlichen im Sinne von Art. 4 DSGVO ein, so dass der GmbH-Geschäftsführer und die Gesellschaft selbst als Gesamtschuldner zur Zahlung von 5.000 Euro Schadensersatz verurteilt wurden.

Urteil des OLG Dresden vom 30. November 2021 – Az: 4 U 1158/21

➢ Weitere interessante Links

Internationale Datentransfers
Eine Handreichung zur Umsetzung der datenschutzrechtlichen Vorgaben bei internationalen Transfers personenbezogener Daten.
https://stiftungdatenschutz.org/fileadmin/Redaktion/PDF/Internationale_Datentransfers/RZ_SDS_Drittlands-Datentransfers_19112021.pdf

Datenschutz bei der Nutzung von Telefax-Diensten
Das Arbeitspapier der Bayerischen Landesbeauftragten für den Datenschutz bietet Bausteine einer Risikoanalyse und zeigt risikomindernde Maßnahmen auf, die bei der Kommunikation mittels Fax zu beachten sind.
https://www.datenschutz-bayern.de/datenschutzreform2018/AP_Telefax.pdf

Beschäftigtendatenschutz | Podcast Folge 29
Bereits mit der Bewerbung beginnen Unternehmen und öffentliche Stellen die personenbezogenen Daten von potenziellen Beschäftigten zu verarbeiten und mit dem Ausscheiden des Mitarbeiters ist die Verarbeitung und Speicherung auch nicht sofort beendet. Die Sächsische Datenschutzbeauftragte Dr. Juliane Hundert hat in diesem Podcast sehr konkrete und praxisrelevante Tipps gegeben.
https://www.datenschutz-praxis.de/verarbeitungstaetigkeiten/beschaeftigtendatenschutz-podcast-folge-29/

Alle Betroffenenrechte der DSGVO in einer Übersicht
Egal ob am Arbeitsplatz, Zuhause am Laptop oder bei Vorlegen der Payback Karte im Supermarkt, überall werden personenbezogene Daten von Betroffenen millionenfach in Umlauf gebracht und verarbeitet. Dennoch sollte und muss man dieses Ausmaß der Datenverarbeitung als Betroffener nicht tatenlos hinnehmen, denn die DSGVO hält eine Reihe effektiver Betroffenenrechte für Sie bereit. Um welche Betroffenenrechte es sich hierbei handelt und wie deren Geltendmachung erfolgen kann, zeigt dieser Artikel.
https://www.dr-datenschutz.de/alle-betroffenenrechte-der-dsgvo-in-einer-uebersicht/

Was besagt das Recht auf Widerruf der Einwilligung?
Der Datenschutz räumt Betroffenen das Recht auf Widerruf der Einwilligung ein. Was dieses Betroffenenrecht besagt und auf sich hat, ist Bestandteil dieses Beitrages.
https://www.dr-datenschutz.de/was-besagt-das-recht-auf-widerruf-der-einwilligung/

Verzeichnis von Verarbeitungstätigkeiten – Tipps zur Umsetzung
Im Geschäftsalltag ist das Verzeichnis von Verarbeitungstätigkeiten oft nur dann ein Thema, wenn etwas im Unternehmen umgestellt wird – neue Software, neue Mitarbeiter, neue Prozesse. Oder wenn unverhofft eine Betroffenenanfrage hereinflattert. Doch auch wenn nichts akut ansteht, sollte gerade in den ruhigen Minuten die Dokumentationspflicht der DSGVO angegangen werden.
https://www.dr-datenschutz.de/verzeichnis-von-verarbeitungstaetigkeiten-tipps-zur-umsetzung/