LOSCHELDER

Newsletter Datenschutzrecht

Juli 2022

Sehr geehrte Damen und Herren,

ein bekanntes Thema wird einmal wieder heiß, wie dieser Tage auch das Wetter: Unternehmen, die Google Tools auf ihrer Website eingebunden haben, sollten diese überprüfen. Dies gilt jedenfalls bei Nutzung von „Google Fonts“, der Schriftartenbibliothek, die bei etlichen Websites mitläuft. Hier drohen aktuell umfangreiche Schadensersatzforderungen.

Erneut „heiß“ sind auch die Facebook-Fanpages und Unternehmenspräsenzen auf anderen Social Media Plattformen: Die Datenschutzaufsichtsbehörden haben einen neuen FAQ dazu veröffentlicht, den wir in Beitrag 2 für Sie zusammenfassen.

Ein neues BGH-Urteil zur Anzeigenwerbung in E-Mail-Postfächern und ein für die tägliche Praxis hilfreicher Leitfaden zum Datenschutzmanagement runden unseren Sommer-Newsletter ab. Im „Zu guter Letzt“ berichten wir wie immer über aktuelle Bußgeldentscheidungen.

Inhalt

Immer wieder Google: Websitegestaltung überprüfen!

Die Tools von Google erleichtern die Websitegestaltung enorm. Gleichzeitig stehen sie im Fokus der Datenschutzbehörden. Aktuelle Entwicklungen gibt es zu Google Analytics und Google Fonts (Schriftartenbibliothek). Was Sie beim Einsatz dieser Tools beachten – und gerade in Bezug auf Google Fonts zeitnah ändern – sollten, erfahren Sie in diesem Artikel.

1. Google Fonts

Zum Jahresbeginn hat das LG München eine folgenreiche Entscheidung getroffen: Es hat einem Websitebesucher einen Schadensersatz i.H.v. 100 Euro gegen den Websitebetreiber zugesprochen, weil dieser Google Fonts eingesetzt und dafür die IP-Adresse des Websitebesuchers an Google übertragen hatte (Urteil vom 20.01.2022 – 3 O 17493/20). Google Fonts bietet Schriftarten für eine optimierte Darstellung der Website an. Um diese anzuzeigen, wird die IP-Adresse des Besuchers an Google übermittelt, wenn Google Fonts nicht lokal auf eigenen Serverkapazitäten eingebunden ist.

Das Gericht sah keine Erlaubnisgrundlage für diese Datenübertragung, so dass es auf einen womöglich unzulässigen Drittstaatentransfer nicht mehr ankam. Solche Erlaubnisgrundlagen enthält Art. 6 DSGVO, etwa die Einwilligung oder überwiegende berechtigte Interessen. Eine Einwilligung kommt beim Einsatz von Schriftartenbibliotheken regelmäßig nicht in Betracht, da die Seite ohne Google Fonts nicht, wie vom Betreiber gewünscht, angezeigt werden kann. Und berechtigte Interessen verneinte das LG München, da es auch andere, weniger datenintensive Lösungen gäbe.

Die Entscheidung zeigt, wie brisant der Einsatz von Online-Tools sein kann. Die Schadensersatzforderungen angeblicher Websitebesucher nehmen aktuell enorm zu. Es ist daher, ungeachtet der Kritikpunkte an der Entscheidung des LG München, anzuraten, Google Fonts von den eigenen Websites zu verbannen (oder lokal einzubinden).

2. Google Analytics

Der Einsatz von Google Analytics löst bereits seit längerem Bedenken bei den Datenschutzbehörden aus (wir berichteten in

unserem Blog und in unserem Newsletter zum Jahresbeginn zu den Anforderungen an Analysedienste generell).

Jüngst hat nun eine weitere Aufsichtsbehörde in einem konkreten Fall den Einsatz von Google Analytics als rechtswidrig eingestuft: Die italienische Aufsichtsbehörde (SA) in einem Verfahren um eine e-commerce Plattform.

Ob die Entscheidung unmittelbar auf den Einsatz von Google Analytics auf eigenen Websites übertragbar ist, hängt entscheidend von der konkreten Ausgestaltung ab:

a. Konfiguration

Im Verfahren der italienischen SA war die fehlende „IP-Anonymisierung" einer der wesentlichen Kritikpunkte der Datenschutzaufsichtsbehörde. Diese sollte stets aktiviert sein, bei neueren Versionen von Google Analytics soll dies standardisiert erfolgen (die Überprüfung bleibt aber dringend anzuraten).

Die italienische Datenschutzbehörde hält die IP-Anonymisierung mit Blick auf die Möglichkeit von Google, die gekürzte IP-Adresse mit weiteren Informationen in ihrem Besitz anzureichern und so die Re-Identifizierung des Nutzers womöglich doch zu ermöglichen, allein allerdings nicht für ausreichend. Eine weitere geeignete technische Maßnahme könnte nach der SA der Einsatz von Datenverschlüsselungsmechanismen während der Übertragung und im Ruhezustand sein. Derartige Zusatzmaßnahmen werden nach unserem Kenntnisstand von Google aktuell noch nicht angeboten.

Zudem ist zu prüfen, ob die „UID" deaktiviert werden kann: In der Ausgangseinstellung wird beim Einsatz von Google Analytics regelmäßig eine einzigartige Kennnummer mit vergeben (UID), die, wie auch im italienischen Verfahren geschehen, eine Identifikation des Browsers oder Geräts des Websitebesuchers ermöglicht. Deaktiviert man diese Funktion, so fällt ein weiteres personenbezogenes Datum weg, das unter Einhaltung des Datenschutzes transferiert werden könnte. Schwieriger wird dann aber auch eine Nachverfolgung einzelner Nutzer über mehrere Endgeräte hinweg.

b. Einwilligungslösung

In dem österreichischen Verfahren war unter anderem problematisch, dass bei der Aktivierung von Google Analytics keine Einwilligung der Websitenutzer verlangt wurde, sondern lediglich die Möglichkeit des Widerspruchs bestand („Opt-Out"). Um datenschutzrechtliche Risiken zu minimieren, ist die Aktivierung von Google Analytics nur mit Einwilligung eines jeden Nutzers zu empfehlen („Opt-In"). Wie dies im italienischen Verfahren gelöst war, ergibt sich aus der Entscheidung nicht eindeutig.

c. Standardvertragsklauseln

Dem italienischen Verfahren lagen, wie auch in den anderen bereits entschiedenen Verfahren, jeweils nur die alten Standardvertragsklauseln zugrunde. Sind die neuen Standardvertragsklauseln 2021 abgeschlossen, verbessert sich die Situation erheblich, da die neuen Standardvertragsklauseln viele Schwachstellen der alten Version ausräumen. Die alten Standardvertragsklauseln laufen zum 27.12.2022 aus, daher sollten sie ohnehin innerhalb des nächsten halben Jahres flächendeckend abgelöst werden. Auch Google nutzt mittlerweile die neuen Standardvertragsklauseln.

Es bleibt damit auch nach der italienischen Entscheidung dabei: Google Analytics steht in der datenschutzrechtlichen Kritik. Ob der Einsatz aber tatsächlich datenschutzrechtswidrig ist, hängt von der Ausgestaltung im Einzelfall ab.

Update: Facebook-Fanpages

Die Aufsichtsbehörden bleiben aktiv in Sachen Social Media: Nachdem erste Prüfverfahren gegen Facebook-Fanpages von Behörden eingeleitet wurden, hat die Datenschutzkonferenz (DSK) nun einen FAQ veröffentlicht. Dieser zeigt eindeutig: Private Unternehmen müssen achtsam bleiben, wenn sie Facebook und andere Social Media Plattformen nutzen.

Nachdem wir in unserem Juni-Newsletter bereits über den Startschuss zur Prüfung öffentlicher Facebook-Fanpages berichtet haben, reagierte die DSK nun mit ihrer Sitzung vom 22.06.2022 erneut auf das große Interesse an Hinweisen zum rechtskonformen Betrieb von Facebook-Fanpages, indem sie eine Liste von oft gestellten datenschutzrechtlichen Fragen und den dazugehörigen Antworten (FAQ) rund um diese Problematik verabschiedete. In dem Beschluss wird unter anderem beantwortet, warum derzeit der datenschutzrechtskonforme Betrieb von Facebook-Fanpages nicht gewährleistet werden kann und welche Schritte für einen dem Datenschutz entsprechenden Einsatz von Facebook-Fanpages notwendig wären.

Auch wenn die Aufsichtsbehörden nun zunächst Verfahren gegen Behörden eröffnen wollen, die Fanpages betreiben, sind private Unternehmen nicht ausgenommen. Es bleibt daher bei der Empfehlung, die Situation weiter eng zu beobachten und im Bedarfsfall den Facebook-Auftritt zu beenden. Die DSK schreibt dazu in ihren FAQ eindeutig:

- Zur Frage 4, ob Facebook-Fanpages „jetzt sofort deaktiviert werden“ müssen: „Kann die Verarbeitung personenbezogener Daten nicht rechtskonform durchgeführt werden, ist der Betrieb einer Facebook-Fanpage rechtswidrig. Die Aufsichtsbehörden haben seit Jahren auf die Probleme hingewiesen. Übergangsfristen kennt die DSGVO nicht.“

- Zur Frage 6, ob dies nur für Behörden und Unternehmen in öffentlicher Hand gilt, verweist die DSK auf die gleiche Geltung der Regeln auch für private Unternehmen. Fanpages der öffentlichen Hand würden aufgrund der Vorbildfunktion nun aber vorrangig in den Blick genommen.

- Schließlich verweist die DSK auch darauf, dass die Erkenntnisse zu Facebook auf andere Social Media Anbieter (z.B. Instagram, Twitter, TikTok) übertragbar sein können, Unternehmenspräsenzen dort wären dann ebenfalls rechtswidrig, setzt sich die Ansicht der Aufsichtsbehörden durch.

Anzeigenwerbung nur noch mit Einwilligung?

Der Bundesgerichtshof hat sich zu Anzeigenwerbung in E-Mail-Postfächern geäußert und auch für diese Art von Werbung ein Einwilligungserfordernis festgestellt. Der Grund: Auch bei solchen Anzeigen handele es sich um Werbung mittels elektronischer Post, daher seien sie, wie E-Mail-Werbung, nur mit Einwilligung des Empfängers zulässig. Das ist diskutabel, aufgrund des nun vorliegenden BGH-Urteils für die Praxis aber vorerst entschieden. Berücksichtigt werden sollte weiter, ob das BGH-Urteil auch für andere Werbeanzeigen im Web gilt.

Wer ein kostenloses E-Mail-Postfach von Anbietern wie GMX, WEB, T-Online etc. nutzt, dürfte auch Anzeigenwerbung im Posteingang kennen. Regelmäßig werden in Postfächern zwei bis drei neu eingegangene E-Mails angezeigt und anschließend eine grau hinterlegte und als Anzeige markierte Werbung. Anschließend wieder zwei, drei E-Mails und dann noch eine Anzeige mit Werbung.

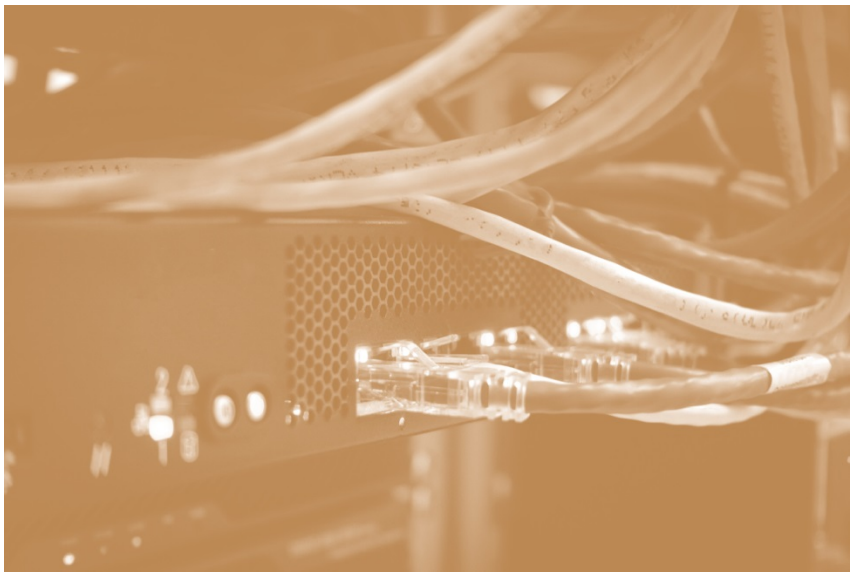
Zu diesen Werbeanzeigen hat sich der Bundesgerichtshof (BGH) in seinem Urteil vom 13.01.2022 – I ZR 25/19 geäußert und im Ergebnis entschieden, dass die Werbung nur mit ausdrücklicher Einwilligung des Nutzers geschaltet werden darf. Rechtlich basiert das auf der Annahme, dass es sich bei Anzeigenwerbung um *„Werbung unter Verwendung elektronischer Post“* handelt, die nach § 7 Abs. 2 Nr. 3 UWG nur mit ausdrücklicher Einwilligung des Adressaten geschaltet werden darf. Das Oberlandesgericht Nürnberg (Urteil vom 15.01.2019 – 3 U 724/18) war noch davon ausgegangen, dass es sich bei den Anzeigen nicht um an den Adressaten versandte Nachrichten und damit nicht um elektronische Post handele. Die Anzeigen seien vielmehr mit normalen Werbebannern auf Websites vergleichbar, für die kein Einwilligungserfordernis bestehe, solange sie nicht personalisiert werden.

Der BGH sah dies, spitzfindig, anders: Er hatte die Frage der Einordnung der Anzeigenwerbung dem Europäischen Gerichtshof vorgelegt (Urteil vom 25.11.2021 – C-102/20) und geht mit diesem davon aus, dass die Anzeigen zwar nicht als elektronische Post einzuordnen seien. Trotzdem handele es sich aber um Werbung, die unter *Verwendung* elektronischer Post, nämlich unter Verwendung des Posteingangs der Empfänger, an diese übermittelt werde. Dies sei ausreichend für die Anwendbarkeit des § 7 Abs. 2 Nr. 3 UWG und daher seien die Werbeanzeigen nur mit Einwilligung zulässig.

Eine wirksame Einwilligung in den Empfang von Anzeigenwerbung setzt voraus, dass der Nutzer explizit einwilligt, Werbung durch Anzeigen im E-Mail-Postfach zu erhalten. Inwiefern eine allgemeine Einwilligung, Werbung zu erhalten oder ein kostenloses Postfach mit Werbung nutzen zu wollen, ausreicht, ist kritisch zu überprüfen und vom Einzelfall abhängig. In dem vom BGH entschiedenen Fall war die Einwilligung zu generell und daher nicht wirksam. Die Nutzer hatten sich lediglich für ein kostenfreies E-Mail-Postfach mit Werbung entschieden, ohne genau informiert worden zu sein, dass auch Anzeigenwerbung im E-Mail-Postfach angezeigt werden soll.

Für Anbieter von E-Mail-Postfächern hat das Urteil zur Folge, dass sie ihre Werbepraxis überprüfen müssen. Anzeigen im E-Mail-Postfach erfordern eine ausdrückliche Einwilligung in die Schaltung. Das Angebot von E-Mail-Postfächern *„gratis, aber dafür mit Werbung“* führt nicht zu einer wirksamen Einwilligung, wenn nicht ergänzend die Details klargestellt wurden, etwa, welche Werbung den Nutzern angezeigt werden soll.

Auf allgemeine Werbeanzeigen im Web wird diese Rechtsprechung indes nicht übertragbar sein, da der BGH gerade auf die Anzeige im E-Mail-Postfach abstellt, die „Verwendung“ elektronischer Post.



Welche Software fürs Datenschutzmanagement?

Die Aufsichtsbehörden bieten praktische Hilfestellungen zur Überprüfung von Datenschutzmanagementsystemen: Mit dem 2019 grundlegend überarbeiteten Standard-Datenschutzmodell (SDM) haben die Datenschutzaufsichtsbehörden des Bundes und der Länder ein Werkzeug bereitgestellt, mit dem für den Bereich des operativen Datenschutzes sichergestellt werden soll, dass eine einheitliche Datenschutz-Beratungs- und Prüfpraxis erfolgt. Der nun veröffentlichte Baustein der SDM-Methode bietet Unternehmen eine praktische Hilfestellung, indem er ihnen eine Anforderungsliste bei der Suche nach geeigneten Datenschutzmanagementsystemen an die Hand gibt.

Die rechtlichen Anforderungen der DSGVO werden durch das SDM in technische und organisatorische Maßnahmen überführt, die sicherstellen sowie den Nachweis dafür erbringen sollen, dass die Verarbeitung personenbezogener Daten nach den Vorgaben der DSGVO erfolgt. Das SDM fungiert also als Unterstützung bei der risikoadäquaten Auswahl und Bewertung solcher Maßnahmen. Dazu werden die rechtlichen Anforderungen der DSGVO den in Art. 5 DSGVO verankerten Gewährleistungszielen Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettung und Intervenierbarkeit sowie der übergreifenden Anforderung der „Datenminimierung“ zugeordnet und ein Referenzmaßnahmen-Katalog bereitgestellt.

Im Referenzmaßnahmen-Katalog werden die zur Erfüllung der gesetzlichen Anforderungen erforderlichen Maßnahmen, unter Zugrundelegung typischer ausgewählter Verarbeitungssituationen, dargestellt und in Bausteinen zusammengefasst. Auf diese Weise werden die abstrakt rechtlichen Vorgaben in konkrete technische und organisatorische Maßnahmen übersetzt. Mit Hilfe des Katalogs kann dann von Unternehmen überprüft werden, ob bei der jeweiligen Verarbeitung von Daten das rechtlich geforderte „Soll“ von Maßnahmen mit dem vor Ort vorhandenen „Ist“ von Maßnahmen übereinstimmt. Bei jeder Verarbeitung ist dabei auch sicherzustellen, dass die Risiken und Rechte für die Freiheiten der von der Verarbeitung betroffenen natürlichen Personen so weit eingedämmt werden, dass ein dem Risiko angemessenes Schutzniveau gewährleistet wird.

Mit dem nun veröffentlichten Anforderungskatalog für ein SDM Tool sollen die wesentlichen fachlichen Hauptfunktionen eines SDM-Tools („Tool“) aus Sicht des Datenschutzes dargestellt werden.

Nach dem Katalog der Datenschutzaufsichtsbehörden sollen Unternehmen bei der Suche eines geeigneten Datenschutzmanagementsystems folgende fachliche Hauptfunktionen berücksichtigen:

1. Dokumentation datenschutzrechtlicher Nachweise („Output-Sicht“ des Tools)

2. Die Durchführung datenschutzrechtlicher Prozesse („Assistenten-Sicht“ des Tools)

3. Anforderungsbereich: Externe Bausteine werden im Tool bereitgestellt („Externe Quellen-Sicht“ des Tools)

4. Anforderungsbereich: Schnittstellen zu anderen Fachverfahren werden bereitgestellt („Schnittstellen-Sicht“ des Tools)

5. Anforderungsbereich: Weitere, allgemeine Anforderungen werden angeboten („Effizienz-Sicht“ des Tools)

Die Ergänzung des SDA um einen weiteren Baustein bietet Unternehmen also bei der Suche nach geeigneter Software erste gute Anhaltspunkte und erleichtert damit das Datenschutzmanagement.

Zu guter Letzt

Die Bußgeldentscheidungen aus diesem Monat stammen allesamt aus dem Ausland. In Deutschland ist es dagegen derzeit ruhig. Die dänische Datenschutzbehörde empfahl ein Bußgeld gegen einen Buchclub, der die Daten abgemeldeter Mitglieder weiter gespeichert hatte. In Italien erhielt ein Krankenhaus für die Offenlegung der Empfänger eines E-Mail-Newsletters ein Bußgeld über 70.000 € und die französische Datenschutzbehörde verhängte ein Bußgeld über eine Million Euro gegen einen Energieversorger, der Kunden ohne Einwilligung angerufen und Betroffenenanfragen unbeantwortet gelassen hatte.

- **Dänemark: Buchverlag unterließ Löschung von 685.000 abgemeldeten Mitgliedern.**

Die dänische Datenschutzbehörde empfahl ein Bußgeld in Höhe von 134.427 Euro gegen den dänischen Verlag Gyldendal, weil er die personenbezogenen Daten seiner abgemeldeten Buchclub-Mitglieder nicht gelöscht hatte.

Während eines Inspektionsbesuchs bei Gyldendal A/S stellte die dänische Datenschutzbehörde fest, dass das Unternehmen Informationen von über 685.000 nicht angemeldeten Mitgliedern des Buchclubs von Gyldendal länger als nötig aufbewahrte. Die Daten wurden von dem Buchclub auf einer „passiven Datenbank" gespeichert, welche keine Verfahren oder Leitlinien für die Löschung der Daten aufwies. Einige dieser Informationen wurden so länger als zehn Jahre aufbewahrt.

Die Datenschutzbehörde stellte anschließend fest, dass Gyldendal gegen die Grundsätze der Speicherbegrenzung und der Rechenschaftspflicht verstieß, indem die personenbezogenen Daten einer Vielzahl von betroffenen Personen länger als erforderlich aufbewahrt wurden. Daher zeigte sie den für die Verarbeitung Verantwortlichen bei der Polizei an und empfahl eine Geldstrafe in Höhe von 134.427 Euro.

Die dänische Datenschutzbehörde verhängt nicht direkt Bußgelder, sondern verweist solche Fälle an die Polizei. Diese prüft dann, ob Gründe für eine Anklageerhebung vorliegen. Über eine mögliche Geldstrafe entscheidet ein Gericht.

- **Italien: 70.000 Euro Bußgeld für ein italienisches Krankenhaus, aufgrund einer falschen „CC–Setzung" beim Newsletter-Versand.**

Grund für das Bußgeld war, dass das Krankenhaus Società Ospedale San Raffaele Srl beim Versand zweier medizinischer Newsletter die Empfänger fälschlicherweise in CC statt BCC gesetzt hatte. Hierdurch wurden die personenbezogenen Daten an alle Empfänger weitergegeben. Da dies ohne rechtliche Grundlage erfolgte, verhängte die italienische Datenschutzbehörde ein Bußgeld von 70.000 Euro.

Es handelte sich dabei um einen Newsletter mit 499 und einen weiteren mit rund 90 Empfängern. Nachdem das Krankenhaus die Verletzung gemeldet hatte, führte es an, dass kein konkretes Risiko für die betroffenen Personen aufgrund des kleinen Empfängerkreises bestünde. Zudem enthielten 193 E-Mail-Adressen keine Hinweise auf Namen und stellten demnach keine personenbezogenen Daten dar. Nach dem Verstoß wurden neue technische und organisatorische Maßnahmen getroffen, um die Datensicherheit zu gewährleisten.

Die Datenschutzbehörde stellte hingegen fest, dass bereits E-Mail-Adressen an sich personenbezogene Daten seien, auch ohne Bezug auf Namen. Da die Newsletter zudem an Patienten der betreffenden medizinischen Einrichtung gesendet wurden, konnten so mögliche Rückschlüsse auf die Gesundheit der Betroffenen gezogen werden.

Die Datenschutzbehörde sah in der Weitergabe personenbezogener Daten, einschließlich Gesundheitsdaten, ohne Rechtsgrund an Dritte einen Verstoß gegen Art. 5 f und Art. 9 DSGVO. Bei der Festsetzung der Geldbuße wurde jedoch der unbeabsichtigte Charakter des Verstoßes, die im Nachhinein ergriffenen Maßnahmen zur Verhinderung einer Wiederholung und die Tatsache, dass der für die Verarbeitung Verantwortliche mit der Datenschutzbehörde zusammengearbeitet hatte, berücksichtigt.

- **Frankreich: Das im Jahr 2020 von der CNIL gegen Amazon verhängte Bußgeld von 35 Millionen Euro wurde vom Staatsrat bestätigt.**

Im Urteil vom 27.06.2022 bestätigt der Staatsrat die von der französischen Datenschutzbehörde CNIL im Jahr 2020 gegen

Amazon Europe Core verhängte Strafe von 35 Millionen Euro. Hintergrund des damals auferlegten Bußgeldes war, dass das Unternehmen Cookies auf den Computern der Nutzer ohne deren vorherige Zustimmung oder ausreichende Informationen abgelegt hatte.

In ihrer damaligen Entscheidung stellte die CNIL zwei Verstöße gegen Art. 82 des französischen Datenschutzgesetzes fest. Beim Besuch der Website "Amazon.fr" wurden automatisch und ohne Zutun des Nutzers eine große Anzahl von Cookies mit Werbezweck auf dem Computer abgelegt. Diese Art von Cookies war jedoch für den Dienst nicht zwingend erforderlich. Zudem ermöglichten die auf der Website angezeigten Banner dem Nutzer nicht, klar im Voraus über die Hinterlegung von Cookies informiert zu werden, insbesondere über den Zweck dieser Cookies und die Möglichkeiten, sie abzulehnen.

Der Staatsrat bestätigte nun die vergangene Entscheidung der CNIL und damit einhergehend die Verstöße durch Amazon und die Höhe des Bußgeldes. Er erinnerte daran, dass die CNIL für die Verhängung von Sanktionen bei Verstößen gegen Art. 82 des französischen Datenschutzgesetzes auch dann zuständig sei, wenn der für die Verarbeitung Verantwortliche zwar nicht in Frankreich ansässig ist, jedoch über eine Niederlassung auf französischem Staatsgebiet verfügt, welche an Tätigkeiten im Zusammenhang mit der durchgeführten Verarbeitung beteiligt ist.

- **Frankreich: Die CNIL verhängt ein Bußgeld in Höhe von einer Millionen Euro gegen TotalEnergies Électricité et Gaz France.**

Bei der französischen Aufsichtsbehörde gingen zunächst mehrere Beschwerden ein, denen zufolge der französische Energieerzeuger und -versorger TotalEnergies Électricité et Gaz France Anfragen von Nutzern bezüglich des Zugangs zu ihren Daten unbearbeitet ließ. Zudem wollten diese sich gegen den Erhalt von Anrufen zu Zwecken der Direktwerbung zur Wehr setzen.

Es stellte sich daraufhin heraus, dass der Nutzer beim Ausfüllen eines Webformulars für die Anmeldung zu einem neuen Vertrag keine Möglichkeit hatte, der Weiterverwendung seiner Daten zum Zwecke der kommerziellen Werbung für ähnliche Produkte oder Dienstleistungen zu widersprechen. Dies verstößt jedoch gegen die

französischen Rechtsvorschriften. Zudem lag somit ein Verstoß gegen die Art. 12, 14, 15, 21 DSGVO vor.

Nach Bekanntwerden der Beschwerden unternahm das Unternehmen die erforderlichen Maßnahmen, um den Mangel zu beheben, was bei der Festsetzung des Bußgeldes berücksichtigt wurde.

Für alle weiteren Fragen rund um das Datenschutzrecht stehen Ihnen gerne zur Verfügung

Dr. Kristina Schreiber
+49(0)221 65065-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
+49(0)221 65065-200
simon.kohm@loschelder.de

Dr. Malte Göbel
+49(0)221 65065-337
malte.goebel@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de