IN DIESER AUSGABE:

Newsletter August 2023

Datenschutz

Liebe Leserinnen und Leser,

in unserem Newsletter möchten wir Sie konkret auf Themen aufmerksam machen, die in der Praxis immer wieder gern für Fragen oder Verwirrung sorgen. Auch wenn wir an dieser Stelle nur einen kurzen informativen Überblick geben können, stehen wir Ihnen gerne beratend zur Seite.
Viel Spaß beim Lesen!

Ihre ANMATHO AG

Handlungsbedarf beim Einsatz von Google Analytics

Die Organisation NOYB (bekannt durch den Datenschutzaktivisten Max Schrems) hat bei den zuständigen Aufsichtsbehörden 2020 gegen Unternehmen, die Google Analytics und Facebook Connect einsetzten, Beschwerde eingelegt. Dabei ging es darum, dass bei der Übermittlung von personenbezogenen Daten in die USA kein angemessenes Datenschutzniveau gewährleistet ist (Verstoß gegen Art. 44 ff. DSGVO).

Die schwedische Datenschutzbehörde IMY (https://www.imy.se/en/news/four-companies-must-stop-using-google-analytics/) hat jetzt ein Bußgeld von ca. 1 Mio. € gegen das Telekommunikationsunternehmen Tele2 verhängt. Das Unternehmen hat die Übermittlung der Daten an das Drittland auf Standardvertragsklauseln gestützt, aber nach Ansicht der Behörde nicht für ein ausreichendes Maß an Schutzmaßnahmen gesorgt.

Seit dem 1. Juli 2023 hat Google den Dienst Google Analytics auf die Version Google Analytics 4 umgestellt. Neben einigen Features soll es auch mehrere datenschutzfreundlichere Konfigurationen geben, wie z.B. die Speicherung der Daten auf EU-Servern und die voreingestellte Anonymisierungsfunktion. Weiterhin gibt es wohl auch die Möglichkeit, ein paar Einstellungen vorzunehmen, die das Tracking begrenzen.

Da auch die deutschen Aufsichtsbehörden den Datentransfer in Drittländer - gerade im Hinblick auf Google Analytics - prüfen, sollten Unternehmen Vorsicht walten lassen. Eventuell sollte man einen Wechsel auf ein anderes Tool in Betracht ziehen oder zumindest entsprechende Maßnahmen zum Schutz der personenbezogenen Daten ergreifen.

Neue Impulse erhält das Thema auch durch die aktuelle Entscheidung der EU-Kommission, die für die USA einen Angemessenheitsbeschluss gefasst haben (siehe diesbezüglich den Artikel in diesem Newsletter). Das sollte aber nicht als Freifahrtschein verstanden werden, da der Angemessenheitsbeschluss zum Einen an gewisse Bedingungen geknüpft ist und zum Anderen mit ziemlicher Sicherheit wieder vor dem EuGH landen wird.

Neues zum Trans-Atlantik Data Privacy Framework (TADPF)

Gegen die Empfehlung des EU-Parlaments vom 11. Mai 2023 hat die EU-Kommission am 10.07.2023 überraschend den lange herbeigesehnten „Angemessenheitsbeschluss“ für den Datenschutzrahmen zwischen der EU und den USA erlassen. Der neue Angemessenheitsbeschluss erlangte direkt mit seiner Annahme am 10. Juli 2023 Rechtskraft.

Seitdem der Europäische Gerichtshof (EuGH) vor drei Jahren die Durchführungsverordnung zum Privacy Shield Abkommen zwischen den USA und der EU für unwirksam erklärt hat, war der Austausch von personenbezogenen Daten und die Nutzung von Diensten großer US-Anbieter wie z.B. Microsoft kaum rechtlich zulässig möglich. Unternehmen, Schulen und Universitäten sahen sich mit den Anforderungen überfordert, die beispielsweise beim Einsatz von Microsoft 365 zu beachten waren.

In dem Angemessenheitsbeschluss, der auf dem Trans-Atlantik Data Privacy Framework (TADPF) basiert wird festgelegt, dass die Vereinigten Staaten ein angemessenes Schutzniveau – vergleichbar mit dem der Europäischen Union – für personenbezogene Daten gewährleisten, die innerhalb des neuen Rahmens aus der EU an US-Firmen übermittelt werden.

Somit dürfen an US-Unternehmen, die sich über einen webbasierten Selbstzertifizierungsprozess an die Anforderungen des TADPF binden, wieder personenbezogene Daten übermittelt werden. Seit dem 17. Juli 2023 können sich Unternehmen auf der Internetseite des US-Handelsministeriums zertifizieren lassen. Dort soll auch für alle einsehbar sein, welche Unternehmen bereits zertifiziert sind.

Die „alten“ Zertifizierungen nach dem Privacy Shield gelten erst einmal weiter. Zertifizierte Unternehmen müssen ihre privacy policies innerhalb von drei Monaten nach Inkrafttreten des Beschlusses so anpassen, dass sie auf das neue Framework verweisen Die Diskussion um die rechtskonforme Nutzung von Office365 usw. sollte damit zunächst ein Ende haben.

Es ist aber davon auszugehen, dass das neue Abkommen auch zur richterlichen Überprüfung vor dem EuGH landen wird. Schon während des Abstimmungsprozesses für den Angemessenheitsbeschluss gab es Kritik aus verschiedenen Richtungen, unter anderem auch vom EU-Parlament. Kritiker führen an, das Abkommen sei im Wesentlichen eine Kopie des Privacy Shields. Auch besteht die Gefahr, dass nach der nächsten US-Wahl die Executive Order von Präsident Biden zurückgezogen wird. Diese Order schreibt Zusagen für EU-Bürger im Zusammenhang mit Massenüberwachungen in den USA vor, und beschneidet die Befugnisse der Geheimdienste bezüglich des Datenschutzes für Nicht-US-Bürger. Diese Order ist eine wesentliche Grundlage der Vereinbarung.

Internet-Präsenz - Datenschutz-Hinweise und Einwilligungen

Die Datenschutzgesetze verpflichten die Unternehmen zur Einhaltung einer ganzen Reihe von Regelungen zum Schutz der personenbezogenen Daten. Neben einer wirksamen Rechtsgrundlage und dem angemessenen technischen und organisatorischen Schutz der personenbezogenen Daten zählen hierzu insbesondere auch **Pflichten über die Information der Betroffenen** (Art. 12, Art. 13, Art. 14 DSGVO).
Diese Informationsverpflichtung gilt für das Unternehmen auch im Zusammenhang mit dem Angebot einer Webseite, z.B. zu Werbezwecken, für die Annahme von Bestellungen oder für die Nutzung eines Kundenkontos.

Einfach und Verständlich - Datenschutz-Hinweise
Dieser Informationspflicht kann in der Regel relativ einfach nachgekommen werden. Am zweckmäßigsten werden alle datenschutzrelevanten Information auf einer Seite der Webseite mit ‚**Datenschutz-Hinweisen**' zusammengefasst und in verständlicher Form präsentiert. Zielgruppe dieser Hinweise sind eben nicht Juristen oder ITler, sondern die Besucher der Internetseite.
Der Teufel liegt hier aber im Detail. Neben Angaben zur verantwortlichen Stelle, den Kontaktdaten des Datenschutzbeauftragten und den Rechten des Seitenbesuchers sind insbesondere alle durch die Webseite genutzten Verfahren und der Umfang der jeweiligen Datennutzung sorgfältig zu beschreiben. Soweit für die Verfahren Dienstleister eingesetzt werden oder wenn es sich um Anwendungen von Dritten handelt, sind diese zu benennen.
Unvollständige oder falsche Angaben können hier schnell zu **bußgeldbewerten Abmahnungen** der Aufsichtsbehörden führen. Die Aufsichtsbehörden haben konkrete Hilfestellungen veröffentlicht, welche Inhalte in den Datenschutz-Hinweisen enthalten sein sollten (z.B. https://www.ldi.nrw.de/datenschutz/medien-und-technik/websites-muster-fuer-datenschutzhinweise).
Für die Datenspeicherung und den Datenaustausch zwischen dem Seitenbesucher, dem Webseitenbetreiber und ggf. den genutzten Dienstleistern kommen in der Regel sogenannte **Cookies** zum Einsatz. Das sind kleine Textdateien, die auf dem Endgerät des Seitenbesuchers von den jeweiligen Verfahren abgelegt und dort vom Seitenbetreiber oder den Dienstleistern abgerufen werden können.

Rechtsgrundlagen für Datennutzung und Einwilligungen
Die Nutzung und Speicherung von personenbezogenen Daten erfordert auch im Zusammenhang mit einem Internetauftritt die Erfüllung der strengen Richtlinien hinsichtlich der Berechtigung und Notwendigkeit zur Datennutzung. Die Datenschutzgrundverordnung setzt einen festen Rahmen für die möglichen Rechtsgrundlagen (Art. 6 Abs. 1 DSGVO) und verlangt, dass die jeweils angewendete Rechtsgrundlage für jedes Verfahren explizit aufgeführt und - soweit sinnvoll - erläutert wird.
Im Zusammenhang mit dem Internetauftritt werden vor allem Verfahren genutzt, die dem ‚berechtigten Interesse des Seitenbetreibers' (Art. 6 Abs. 1 lit. f DSGVO) z. B. die ‚essentiellen Cookies' oder die zur Erfüllung vertraglicher Verpflichtungen (Art. 6 Abs. 1 lit. b DSGVO) des Seitenbetreibers dienen (z.B. Kontoabwicklung, Bestellungen).
Mangels anderer Rechtsgrundlagen werden sehr häufig **Einwilligungen** (Art. 6 Abs. 1 lit. a DSGVO) vom Seitenbesucher eingeholt. Je nach Funktionsumfang der Internetseite kann hierbei eine große Anzahl von Einzelabfragen erforderlich sein. Um den Dialog für die Seitenbesucher zu vereinfachen, kommen hierfür sogenannte ‚Consent-Tools' oder ‚Cookie-Banner' zum Einsatz.

Der **Cookie-Banner** listet die einzelnen Cookies in verschiedenen Gruppierungen auf (z.B. ‚unverzichtbare Cookies', ‚Werbung', ‚Social Media') und gibt dem Seitenbesucher die Möglichkeit, eine Einzel- oder eine Gruppenauswahl zu treffen.
Die Einholung von Einwilligungen unterliegt strengen gesetzlichen Regelungen (Art. 7 DSGVO). Um den Dialogablauf gesetzeskonform zu gestalten, müssen daher einige **Regeln** beachtet werden.

- Im Dialog muss explizit eine ‚Ablehnungsschaltfläche' vorhanden sein.
- Die Ablehnung darf nicht dadurch erschwert werden, dass umständliche Mehrfachklicks ausgeführt werden müssen.
- Die Gestaltung der Dialogseite darf nicht dazu führen, dass der Seitenbesucher dazu ‚überredet' wird, seine Zustimmung zur Einwilligung zu geben (‚Nudging') z.B. durch verschiedene Farben, unterschiedliche Schriftgrößen etc.

Falls eine Einwilligung aufgrund von Fehlern nicht wirksam wird, besteht die Gefahr, dass die Speicherung der personenbezogenen Daten in dem betreffenden Verfahren nicht statthaft ist. Diese fehlende Rechtsgrundlage kann von Aufsichtsbehörden mit erheblichen Bußgeldern belegt werden.

PIMs - Personal Information Manager
Im Telekommunikation-Telemedien-Datenschutzgesetz (§26 TTDSG) hat der Gesetzgeber 2021 den Raum geschafften, um die unübersehbar werdende Landschaft an **Consent-Tools**, Cookie-Bannern und Einwilligungsdialogen zu vereinfachen und zu standardisieren. Idee ist es hierbei, separate Dienste (Personal Information Manager, PIMs) im Internet anzubieten, in denen die Internetnutzer ihre Einwilligungen zu bestimmten Nutzungsbereichen einmalig geben können. Die einzelnen Internetseiten greifen dann im Hintergrund wiederum auf die in diesem Dienst hinterlegten Einwilligungen zurück.
Aufgrund regulatorischer Unzulänglichkeiten gibt es diese Dienste heute noch nicht. **Der Gesetzgeber plant** aber die notwendigen Details der Einwilligungsverwaltung durch externe Dienste in einer Verordnung zu regeln. Wir werden darüber weiter berichten.
Bei der Gestaltung der Datenschutz-Hinweise auf der Internetseite und bezüglich der Consent-Tools und Cookie-Banner stehen die Berater der ANMATHO AG mit ihrer Praxiskompetenz gerne zur Verfügung.

Wenn Sie Interesse an weiteren Informationen zu den vorgestellten Themen haben, wenden Sie sich gern an Ihren Datenschutzbeauftragten der ANMATHO AG oder an info@anmatho.de.