Topaktuelles DSGVO-Update zu Google Analytics und Datenaustausch mit UK

Plus TOMs, Teil 2. Haben Sie alles DSGVO-konform erfüllt?

Im vorigen BAV-Newsletter (hier nachlesen…) berichteten wir darüber, dass die **portugiesische Datenschutzbehörde eine Megastrafe** über ein Spital verhängt hatte, weil die Behörde **Verfehlungen bei den TOMs, also den technischen und organisatorischen Maßnahmen,** die im Zuge der DSGVO-Umsetzung realisiert werden mussten, feststellte.

Konkret musste das Unternehmen **EUR 400.000** bezahlen. Die Strafe war nur **deshalb „so gering"**, weil man sich kooperativ gegenüber der Behörde zeigte und aktiv an der Behebung der Mängel mitgearbeitet wurde. Dennoch musste diese Strafe tatsächlich bezahlt werden.

Und wir erklärten, was man genau unter den TOMs (Abkürzung für „**T**echnische und **O**rganisatorische **M**aßnahmen") versteht und zwar konkret unter der Zutritts-, Zugangs-, Zugriffs- und der Weitergabekontrolle.

Heute sehen wir uns die **4 weiteren TOMs-Bereiche**, konkret die Eingabe-, Auftrags-, Verfügbarkeits- und Datentrennungskontrolle, ebenso an wie **wichtige DSGVO-Entscheidungen**, die für Ihre tägliche Arbeit relevant sein könnten.

A) Die TOMs Erklärung, Teil 2:

Die Zutritts-, Zugangs- und Zugriffs- sowie Weitergabekontrolle haben wir im vorigen BAV-Newsletter erklärt. (hier nachlesen…)

Heute sehen wir uns die Eingabe-, Auftrags-, Verfügbarkeits- und Datentrennungskontrolle näher an.

a1) Eingabekontrolle
Über die Eingabekontrolle kann **nachverfolgt** werden, **wer wann Daten ins System eingegeben, verändert, gelöscht** hat. Dadurch kann – zumindest nachträglich – herausgefunden werden, ob und wer Daten manipuliert hat. Deshalb sollten Sie in Ihrem Unternehmen vorab überlegen, wer auf welche Daten wirklich Zugriff benötigt (Nicht allen alles erlauben! Wozu sollte ein Lagerarbeiter auf Lohndaten zugreifen dürfen?) Durch die Vergabe von Nutzernamen/Passwort kann man die Zugriffe genau nachverfolgen. Bereits dieses Wissen um die Nachvollziehbarkeit der Zugriffe wirkt **abschreckend und hilft Missbrauch** von Daten **zu verhindern.**

a2) Auftragskontrolle
Vorab zum Erinnern: Die TOMs werden im **Artikel 32 der DSGVO** definiert. Sowohl **Verantwortliche aber auch Auftragsverarbeiter** haben dafür zu sorgen, dass „geeignete technische und organisatorische Maßnahmen" implementiert sind, die sicherstellen, dass „ein angemessenes Schutzniveau gewährleistet ist".

Der **Verantwortliche** ist die Person, das Unternehmen, die/das **über die Verarbeitung von personenbezogenen Daten entscheidet**. Er ist dafür verantwortlich, dass die Daten der Kunden/Mitarbeiter/Lieferanten etc. bestmöglich geschützt werden.

Der **Auftragsverarbeiter** ist dagegen eine Person/ein Unternehmen, das im Auftrag des Verantwortlichen **personenbezogene Daten verarbeitet**.
Bei der Auftragskontrolle geht es konkret um die **Kontrolle Ihrer Auftragsverarbeiter**, um sicherzustellen, dass diese die Daten exakt nach Ihren Weisungen verarbeiten und alles tun, um die Daten zu schützen.

Tipp 1: Gehen Sie Ihre **Lieferanten-Liste** durch und checken Sie, wer als Auftragsverarbeiter für Sie tätig wird.

Tipp 2: Verlangen Sie **von allen Ihren Auftragsverarbeitern regelmäßig deren TOMs**, um prüfen zu können, ob diese nach wie vor die DSGVO am Radar haben und Maßnahmen zum Schutz Ihrer Daten und die Ihrer Kunden gesetzt haben. Es ist ein Leichtes für die Datenschutzbehörde zu kontrollieren, ob Sie diese formale Voraussetzung erfüllt haben. Falls nicht, gibt es für Sie nichts zu diskutieren und zu argumentieren …

Ein paar Ideen, wer für Sie als Auftragsverarbeiter tätig ist:
Druckerei (produziert ein Mailing mit Ihren Daten), EDV-Techniker, IT-Dienstleister, Software-Lieferant, Werbeagentur, Cloud-Anbieter …

Ausnahmen: KEINE Auftragsverarbeiter sind – trotzdem sie Ihre Daten verarbeiten: Steuerberater, Wirtschaftsprüfer, Anwälte …
Von diesen Firmen benötigen Sie keinen Auftragsverarbeitervertrag (AVV), weil diese Personen/Firmen als **„Berufsgeheimnisträger"** gelten. Bei Steuerberatern kommt noch dazu, dass sie aufgrund ihres Berufsrechts stets **weisungsUNabhängig und eigenverantwortlich** tätig sind. Während das typische Zeichen für Auftragsverarbeiter ist, dass diese weisungsgebunden sind.

a3) Verfügbarkeitskontrolle
Ziel ist, dass die Daten immer verfügbar sind und vor einem zufälligen (wegen Irrtum) oder bewussten (etwa durch Hacker-Angriff) **Löschen geschützt** sind oder im Fall des Falles von einem Back-up wiederhergestellt werden können.

Überlegen Sie sich also eine **Backup-Strategie für Ihr Unternehmen**, idealerweise eine automatische und mehrfache Speicherung **an unterschiedlichen Orten,** um auf Nummer sicher zu gehen. Aber auch **technische** Vorkehrungen wie eine unterbrechungsfreie Stromversorgung (also USV-Gerät), **besondere Feuersicherung** (Feuermelder, Feuerlöscher) bzw. **Klimageräte im und Zugangskontrolle** vor dem Server-Raum können hier wertvolle Hilfe leisten.

a4) Datentrennungskontrolle

Hier geht es darum, dass Daten, die für unterschiedliche Zwecke erhoben wurden, getrennt verarbeitet werden müssen, also **nicht alle Daten eines Kunden zusammengeführt** werden dürfen.

Ein Beispiel in diesem Zusammenhang ist, dass Sie eine **E-Mail-Adresse**, die Sie erhalten haben, um z.B. einen Vertrag für eine **Lebensversicherung** abzuwickeln, nicht dazu verwenden dürfen, um diesem Kunden eine Werbung **für eine Solaranlage**, deren Vertrieb Ihr Unternehmen ebenso übernommen hat, via E-Mail zu senden.

Ein Ausweg in diesem Fall wäre die gute alte Post, also ein Brief mit der Information und Übermittlung Ihres Angebotes.

Wahrscheinlich wird es im Falle einer guten Kundenbeziehung beim oben skizzierten Fall kein Problem geben. Aber juristisch betrachtet gilt: Wenn Sie personenbezogene Daten eines Kunden auch **für einen anderen Zweck verwenden wollen**, brauchen Sie eine entsprechende Rechtsgrundlage. Also die **aktive Einwilligung**

des Kunden, dass Sie seine E-Mail-Adresse für den Newsletter mit allen möglichen Produkten Ihres Unternehmens verwenden dürfen.

B) Google Analytics sendet immer Daten in die USA. Nicht DSGVO-konform.

Zu Google Analytics gibt es eine **topaktuelle Entwicklung**, die wieder für ein wenig mehr Klarheit im Datenschutz sorgt.

Konkret hat der **Datenschutzverein von Max Schrems** namens **noyb** (Abkürzung für none of your business, frei übersetzt: Unsere Daten gehen euch nichts an …) eine **Beschwerde bei der Österreichischen Datenschutzbehörde gegen Google** eingebracht.
In der Beantwortung dieser Beschwerde **hat Google angegeben**, „alle Daten aus seinem Analytics-Dienst in den USA zu speichern und zu verarbeiten", zitiert die Computerwelt.
Die **genaue Beschreibung des Falls** können Sie auf der noyb-Webseite nachlesen und zwar hier …

Bisher hatten die **Datenkraken immer argumentiert**, dass sie einen **Sitz in Irland hätten** und nur diese Tochter die Daten verarbeiten würde, also alles innerhalb Europas bliebe. Diese Argumentation und damit die DSGVO-Konformität ist nach der Google-eigenen Aussage nicht mehr haltbar. ALSO besser **HÄNDE WEG von Google Analytics.**

Nach „Schrems-I", der Aufhebung des **Safe-Harbor-Abkommens**, wurde als „Notlösung" ein neues Abkommen zwischen EU und USA abgeschlossen, der **EU-US Privacy Shield** (übersetzt Datenschutzschild). Damit wollte man wieder Rechtssicherheit im Datenschutz herstellen. Zwar kam es zu einigen Zugeständnissen der US-Regierung, aber nach einer neuerlichen Klage durch Max Schrems und zahlreichen negativen Stellungnahmen wurde auch dieses Abkommen aufgehoben. U.a. äußerte die **„Artikel-29-Datenschutzgruppe"** (ein unabhängiges Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes) heftige Bedenken gegen den Privacy Shield („… es liege weiterhin eine flächendeckende und anlasslose Überwachung der EU-Bürger vor …", zitiert Wikipedia).

Als Konsequenz erklärte der EuGH am 16. Juli 2020 auch den Angemessenheitsbeschluss der EU-Kommission über den EU-US Privacy Shield durch das **Schrems-II**-Urteil für ungültig. Hier zum Nachlesen …

Und nun hat Max Schrems **neuerlich eine Beschwerde bei der österreichischen Datenschutzbehörde gegen Google** eingebracht.
In der Beantwortung dieser Beschwerde **hat Google angegeben,** „alle Daten aus seinem Analytics-Dienst in den USA zu speichern und zu verarbeiten", zitiert die Computerwelt.
Die genaue Beschreibung des Falls können Sie auf der noyb-Webseite nachlesen und zwar hier…

Für die Praxis stellt sich nun die Frage, was dieses Google-Eingeständnis für den Einsatz dieses und anderer **Google-Tools auf Webseiten bedeutet.**

Zum Erinnern: Als Konsequenz aus den oben beschriebenen „Schrems-I und II"-Urteilen gelten die **USA aus Datenschutz-Sicht als unsicheres Drittland.**

Welche Konsequenzen hat das für Webseiten? Das können Sie **hier nachlesen…**

Wer auf Nummer sicher gehen will, sollte auf Google Analytics verzichten!

Denn es ist für Nutzer ganz einfach – etwa durch das **kostenlose Tool Ghostery herauszufinden** – ob bzw. dass **Google Analytics von Ihnen verwendet wird.** Die Software ist als Erweiterung für alle gängigen Browser verfügbar und identifiziert diejenigen Skripte, die **die Privatsphäre oder Anonymität des Nutzers** gefährden. Einfach direkt im Browser nach dieser Erweiterung suchen oder sich z.B. von Chip.de herunterladen. Etwa hier…
Mit diesem Tool wird also Ihre Nutzung von **Google Analytics aufgedeckt und kann zu Beschwerden (etwa von Nutzern aber auch spezialisierter Anwälte) bei der Datenschutzbehörde führen.**

C) Datenaustausch zwischen EU und Vereinigtem Königreich weiter erlaubt

Ebenfalls noch vor der Sommerpause hat die Europäische Kommission beschlossen, dass personenbezogene Daten weiterhin ungehindert aus der Europäischen Union in das Vereinigte Königreich fließen können.

Da man aber nicht weiß, ob das so bleiben wird oder Großbritannien daran etwas ändern wird, ist der **Beschluss auf vier Jahre begrenzt.**
Die Pressemeldung der EU Kommission zum Thema können Sie hier nachlesen…

Für die Praxis bedeutet das, dass Sie weiterhin mit Kunden, Partnern, Lieferanten etc. so verfahren können, **als ob das Vereinigte Königreich nach wie vor in der EU wäre,** weil aktuell auf jeden Fall noch die DSGVO-Bestimmungen gelten, trotzdem es aus der EU ausgetreten ist.

RA Mag. Stephan Novotny
Weihburggasse 4/2/26
1010 Wien

kanzlei@ra-novotny.at

www.ra-novotny.at

Quellen und Mitarbeit: Mag. Stephan Novotny (https://www.ra-novotny.at/), Mag. Günter Wagner, B2B-Projekte für Finanz- und Versicherungsbranche (www.b2b-projekte.at), Newsletter von meineberater.at, Webseite von noyb.eu, Wikipedia, Computerwelt, Pressemeldung EU-Kommission