FAQ Webinar „„Datenkrake“ im Dilemma?“

Achtung: Die FAQ betreffen den Kenntnisstand Februar 2022

1. **Muss ein Cookie-Banner („Cookie-Box“ oÄ) auch beim Tracking ohne Cookies mit der Info „du wirst getrackt“ angezeigt werden?**

Ja. Die Regelungen aus dem Telekommunikationsgesetz 2021 (§ 165 Abs 3 TKG 2021) sind technologieneutral ausgestaltet. Ab dem Zeitpunkt, ab dem Informationen auf dem Endgerät des Users abgelegt werden oder auf Informationen im Endgerät zugegriffen wird, müssen die entsprechenden Informationen angeboten und muss (abgesehen von Ausnahmefällen, in das Setzen notwendig ist, um den Dienst, den der User angefordert hat, anbieten zu können, zB technische Cookies) eine Einwilligung eingeholt werden. Durch Gestaltung eines Cookie-Banners iS eines PopUps ist das meist am einfachsten.

2. **Wird der Google Tag Manager auch als „essenzielles Cookie“ gewertet?**

Der Google Tag Manager wird verwendet, um andere Tools laden zu können, zB Google Analytics. Da bereits durch Verwendung des Tag Managers Daten verarbeitet werden können und Webtools auch ohne diesen geladen werden könnten, ist gehen Experten nicht von der technischen Notwendigkeit des Tag Managers aus. Generell gilt im Moment: Datenweitergabe an große Techkonzerne, welche auch Niederlassungen in den USA haben, sind nach der neusten Entscheidung der Datenschutzbehörden (in Österreich der DSB und in Frankreich der CNIL zu Google Analytics) problematisch zu sehen.

3. **Was ist z.B. bei Facebook-Plugins, wenn man nicht ordnungsgemäß informieren kann, was wirklich mit den Daten bei Facebook passiert und an wen sie weitergeben werden?**

Hat man Zweifel über die Rechtmäßigkeit der Verarbeitung oder kann man nicht über die Verarbeitung bei Facebook informieren, mit dem man gemeinsam für die Verarbeitung verantwortlich ist, ist die Information an den User zum einen mangelhaft, zum anderen wird die Einwilligung aufgrund fehlender Informationen nicht gültig sein.

4. **Anbieter von Cookie Banner wären interessant.**

Es gibt einige sehr gute Anbieter-Vergleiche hier und hier. Die WKO selbst kann aufgrund wettbewerbsrechtlicher Vorgaben keine spezifischen Tools empfehlen. Geachtet werden sollte darauf, dass es ein Anbieter aus der EU oder einem sicheren Drittland ist.

5. **Auf vielen Seiten ist eine Vorauswahl im Cookie-Banner bereits angeklickt. Ist das legitim oder muss der Nutzer definitiv klicken, um den einzelnen Cookies zuzustimmen?**

Es gilt Privacy by Default, d.h. die Einwilligung des Users muss über seine aktive Handlung erfolgen. Vorabgehakte Checkboxen entsprechen keiner freiwilligen aktiven Einwilligung. Manche Banner sind insofern ausgestaltet, als „notwendige Cookies“ (zB Spracheinstellungen, Warenkorb-Cookies oÄ) bereits vorabgehakt sind. Streng genommen ist hier keine Einwilligung nötig, weswegen auch nicht suggeriert werden sollte, dass eine gegeben werden kann, aber es gab dazu noch keine Entscheidung einer Datenschutzbehörde.

6. **Wieso ist der Anbieter „Cookiebot“ in Verruf geraten?**

Es gibt eine Entscheidung des deutschen VG Wiesbaden zum Tool „Cookie-Bot“, wonach der Datenverkehr im Hintergrund mit den USA für unzulässig erklärt wurde (sehr verkürzt). Diese Entscheidung ist wegen Verfahrensfehlern bereits wieder aufgehoben.

7. **Wie sieht eine gute Datenschutzerklärung aus? Gibt es dafür eine Vorlage?**

Hilfestellung finden Sie hier.

8. **Welche Alternativen werden empfohlen?**

Sehr gute Anbieter-Vergleiche finden Sie hier und hier. Die WKO selbst kann aufgrund wettbewerbsrechtlicher Vorgaben keine spezifischen Tools empfehlen.

9. **Welche Maßnahmen plant Google, damit in der EU Google Analytics konform eingesetzt werden kann? Gibt es da schon Ideen dazu?**

Es gibt erste Reaktionen von Google-Legal-Chef Kent Walker, aber noch keine konkreten Ideen für Änderungen.

10. **Braucht es Cookie Banner für Webseiten, wenn kein Tracking eingesetzt wird?**

Wenn keine Informationen auf dem Endgerät des Users abgelegt werden und auch nicht auf Informationen vom User am Endgerät zugegriffen wird (keine Cookies, keine Form von Webtracking, kein device fingerprinting oÄ), dann braucht es auch keinen Cookie-Banner.

11. **Was braucht es, wenn YouTube Videos oder Google Maps eingebunden sind?**

Üblicherweise handelt es sich technisch um Plugins, daher ist die Shariff-Lösung, die von Heise entwickelt wurde, empfehlenswert (Basis: 2-Klick-Lösung mit Information beim ersten und Einwilligung beim zweiten Klick).

12. **Was heißt Einwilligung bei Plugins?**

Der Grundgedanke ist eine „2-Klick-Lösung“, d.h. der User bewegt den Cursor über das Plugin, aktiviert beim 1. Klick die Information („Daten werden an Social Media Betreiber weitergegeben“, etc) und mit dem 2. Klick wird die Einwilligung aktiviert („Ich bin damit einverstanden“, „OK“ oÄ). Diese Lösung wurde technisch durch die Shariff-Lösung von Heise weiter entwickelt.

13. **Webseitenvorlagen/Templates sind meist aus USA werden aber in der EU auf Servern installiert. Ist das auch Problem mit dem Thema USA?**

Solange Templates nur zur Verfügung gestellt werden, nein. Werden dadurch aber auch bereits Tracking-Tools aktiviert, welche einen Datenverkehr mit den USA verursachen, dann ja. Es muss jedenfalls geprüft werden, was konkret auf der Webseite zum Einsatz kommt.

14. **Betrifft die Entscheidung der DSB zu Google Analytics auch die Google Search Console?**

Google Search Console ist ein weiterer Dienst von Google, mit dem die Präsenz Ihrer Website in den Google-Suchergebnissen beobachtet werden könnten, die Basis ist daher der Search Engine und nicht ein Analysetool auf Ihrer Website (so die Beschreibung von Google selbst). D.h. es ist mit keiner Datenübermittlung durch Sie oder Ihre Website an Google verbunden, Sie erhalten lediglich statistische Daten (anonyme oder anonymisierte Daten), weshalb die DSB Entscheidung darauf keine Auswirkungen hat (nach dem derzeitigen offiziellen Kenntnisstand).

15. **Welche Websites betrifft die österreichische Entscheidung nun im ersten Schritt – Seiten, die auf einem österr. Server liegen oder ist das abhängig von der benutzten Domain?**

Die Entscheidung der DSB zu Google Analytics betrifft österreichische Websites, unabhängig vom Serverstandort, wenn diese zB Google Analytics oder andere Tools auf Websites im Einsatz haben, die einen Datenverkehr mit den USA bewirken (und keine ausreichenden technischen / organisatorischen Maßnahmen eingebunden haben). Die (Top-Level-)Domain ist dafür unerheblich.

16. **Muss ich auch wenn ein europäisches Tool verwende einen Cookiebanner (bzw Cookie-Einwilligung) setzen?**

Auch bei europäischen Tracking-Tools ist ein Cookie-Banner, d.h. eine Information über das Tracking, und eine Einwilligung nötig.

Achtung: Die DSB Entscheidung zu Google Analytics beschäftigte sich nicht mit dem Cookie-Banner!

17. **Gibt es bei Amazon Market Place internationalen Datenaustausch?**

Die Frage ist leider ungenau. Grundsätzlich ist es möglich, dass auf dem Marktplatz Daten auch international ausgetauscht werden. Es hängt von den unterschiedlichen Anbietern ab, aber auch von den Tools, die Amazon im Einsatz hat.

18. **Wo ist es geregelt, dass eine Übermittlung mit Zustimmung zulässig ist?**

Der internationale Datenverkehr ist auf Basis einer informierten Einwilligung in Ausnahmefällen in ein unsicheres Drittland denkbar:

Art. 49 Abs 1 lit a DSGVO

„(1) Falls weder ein Angemessenheitsbeschluss nach Artikel 45 Absatz 3 vorliegt noch geeignete Garantien nach Artikel 46, einschließlich verbindlicher interner Datenschutzvorschriften, bestehen, ist eine Übermittlung oder eine Reihe von Übermittlungen personenbezogener Daten an ein Drittland oder an eine internationale Organisation nur unter einer der folgenden Bedingungen zulässig:

a) die betroffene Person hat in die vorgeschlagene Datenübermittlung ausdrücklich eingewilligt, nachdem sie über die für sie bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde.“

Achtung: Ob eine solche ausdrückliche, konkrete Einwilligung auch pauschal von allen Website-Besuchern eingeholt werden kann, ist strittig und wird z.B. vom Europäischen Datenschutzausschuss kritisch gesehen (vgl. EDSA Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679).

19. **Wie sieht es mit Diensten wie GoogleFonts oder Google ReCaptcha aus? Bedürfen diese Dienste auch eine vorherige Zustimmung?**

Ja. Zumindest zu GoogleFonts gibt es eine erste Entscheidung in Deutschland.

20. **Beim Einsatz von Matomo / Piwik analytics im No-Cookie-Modus ist kein Cookie-Banner nötig?**

Bei Analysetools, die personenbezogene Daten verarbeiten, ist eine Information und eine Einwilligung nötig. Offen bleibt noch, ob hier etwaig mit der Ausnahme „notwendig, um einen Dienst, den der User angefordert hat, zu erbringen“ argumentiert werden kann (Reichweitenmessung auf Websites als notwendig, um sinnvolle Informationen anzubieten). Die französischen und deutschen Aufsichtsbehörden erarbeiten zu diesem Thema gerade Leitfäden.

21. **Wie schaut es jetzt mit Zahlungsanbieter wie Stripe aus? Fallen diese jetzt auch unter die Problematik?**

Stripe ist ein Zahlungsdienst, der auf Webseiten eingebunden werden kann. Stripe führt nach eigenen Informationen (vgl Datenschutzinformationen von Stripe) einen Datenverkehr in die USA auf Basis der Standardvertragsklauseln durch. Ob diese und weitere technische / organisatorische Maßnahmen im Einzelfall ausreichend sind, um die personenbezogenen Daten der Kunden zu schützen, ist derzeit noch nicht bekannt, da es noch keine Untersuchung durch eine Datenschutz-Aufsichtsbehörde gegeben hat.

22. Welche Unterschiede gibt es Österreich-Deutschland?

Rechtlich gilt die DSGVO und die jeweiligen nationalen Umsetzungen der ePrivacy-Richtlinie – in Österreich demnach das Telekommunikationsgesetz 2021 und in Deutschland das Telekommunikation-Telemedien-Datenschutz-Gesetz. Inhaltlich gibt es keine nur wenige Unterschiede.

23. Was genau sind zusätzliche technische Maßnahmen?

Technische Maßnahmen, wie z.B. Pseudonymisierung, Verschlüsselung oder Anonymisierung (vgl. EDSA Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679).

24. Ist der Google Ads Tag ebenso von dieser Entscheidung betroffen?

Ja.

25. Muss der Cookie-Banner die Seite verdeckt/blockiert bevor der User auf die Seite kommt?

Es dürfen keine Cookies, außer jene, die für die Funktionalität der Website notwendig sind, gesetzt werden, bevor der User seine Einwilligung dazu gibt. D.h. es gibt keine Vorgaben an die Gestaltung des Banners iSv wie groß dieser zu sein hat. Es ist in Ihrem Sinne, dass der User schnell sieht, dass er auch Cookies zustimmen kann und Sie diese dann setzen dürfen. Ist der Banner zu klein und der User klickt nicht auf die Einwilligung, können Sie auch die Cookies nicht aktivieren.

26. **Ist der Betreiber der Webseite (der Kunde) oder der Webdesigner verantwortlich für die Rechtmäßigkeit?**

Wenn der Designer / die Agentur den Kunden ausreichend (bestenfalls schriftlich, z.B. per Mail) informiert und gewarnt hat, ist der Websitebetreiber / der Kunde verantwortlich.

27. Darf man bestehende Daten aus z.B Analytics oder einem Newsletter-Tool in ein anderes Europäisches Tool übernehmen?

Das richtet sich nach den Nutzungsbedingungen der jeweiligen Anbieter. Fraglich ist auch die Kompatibilität.

28. Könnte die WKO einen Datenschutzgenerator anbieten?

Das tun wir bereits: Online-Ratgeber zu Informationspflichten mit individualisierter Datenschutzerklärung am Ende.

29. Wie unterschiedlich ist deutsches und österreichisches Recht, wenn Generatoren verwendet werden?

Bei Web-Generatoren von Datenschutzerklärungen muss auf das Urheberrecht – in Ö wie in Dtl – geachtet werden. Manche Generatoren sind kostenpflichtig, manche zitierpflichtig. Das richtet sich nach dem jeweiligen Generator und nicht nach dessen Herkunftsland.

30. **Mit GA4 sind die Daten anonymisiert – ist man dann mit Cookie Banner mit Ablehnbutton auf der sicheren Seite?**

Nein. Nach derzeitiger Einschätzung von Experten zur Entscheidung der DSB ist auch Google Analytics in der 4er Version nicht DSGVO-konform, da keine vollständige Anonymisierung der Informationen der User vor Übermittlung an Google erfolgt.

31. **Die bayrische Datenschutzbehörde untersagte im vergangenen Jahr den weiteren (ungeprüften) Einsatz der Marketing-Plattform „Mailchimp". Blüht uns das in Österreich demnächst womöglich auch?**

Deutsche Aufsichtsbehörden scheinen derzeit strenger zu agieren als unsere österreichische DSB. Möglich ist es grundsätzlich, dass auch hierzulande mehr Verfahren zum Einsatz von Tools gibt, welche einen Datentransfer in die USA gewährleisten.

Anmerkung: Je stärker europäische Alternativen nachgefragt werden, desto größer ist der Markt und desto besser üblicherweise auch das Angebot.

32. **Hab ich das richtig verstanden, sobald Server-Logfiles aktiviert sind, muss ich den Besucher für Tracking einwilligen lassen?**

Server-Logfiles werden nicht zwingend zum Tracken von User eingesetzt, vielmehr zum Auffinden problematischer Aktivitäten oder Probleme von Websites. Das würde unter die Kategorie „technisch notwendig" fallen und wäre demnach keine Einwilligung erforderlich, aber dennoch eine Information der User.

33. **Wie kann ich prüfen, ob persönlichen Daten an Google gesendet – auch zB über die URL?**

Jede Anfrage einer Website (die Eingabe der URL im Browser) löst einen Datenverkehr aus. Dieser ist jedoch notwendig, sodass die Seite überhaupt in Ihrem Browser angezeigt werden kann und daher nicht an eine Einwilligung über den Websitebetreiber gebunden (das wäre auch kaum bewerkstelligbar). Welcher Datenverkehr dann über die Seite selbst ausgelöst wird und ob Cookies oÄ im Einsatz sind, kann über die Datenschutzeinstellungen im jeweiligen Browser herausgefunden werden.

34. **Reicht „anonymize IP" als technische Maßnahme aus?**

Nein. Auch andere Informationen, die über Tracking eingeholt werden, gelten nach der Entscheidung der DSB als personenbezogen (zB Informationen über Browser, Plugins, Spracheinstellungen etc).

35. **Wir sprechen hier nur über GA. Eigentlich gilt das aber sinngemäß auch für reCaptcha, Google Fonts und Google Maps. Auch die werden oft automatisch und unreflektiert mit Templates ausgeliert. Wir hier vom Schweregrad unterschieden?**

Nein, es gibt keine Unterscheidung im Schweregrad.

36. **Kann man Vimeo statt YouTube einbinden?**

Auch Vimeo hat Niederlassungen in den USA, weshalb ein Datentransfer nicht ausgeschlossen werden kann. Ob ausreichend technische oder organisatorische Maßnahmen getroffen werden, ist derzeit nicht bekannt bzw gibt es noch keine Einschätzung einer Aufsichtsbehörde dazu.

37. **Worauf stützt sich die Aussage, dass die Einwilligung für Datenübermittlung in die USA nur in Ausnahmefällen (also nicht routinemäßig) als Grundlage verwendet werden darf?**

Zum einen geht es aus der Überschrift des Art. 49 bereits hervor („Ausnahmen für bestimmte Fälle“. Zum anderen handelt es sich um eine Einschätzung vom Europäischen Datenschutzausschuss, der die Einwilligung nur für gewisse Fälle anwendbar macht (vgl. EDSA Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679).

38. **Wie soll man zukünftig mit Newsletter-Tools umgehen, die Daten in die USA senden? Standardvertragsklauseln sind bei einigen Anbietern vermutlich nicht durchsetzbar. Eine EU-Alternative kommt nicht in Frage, da diese Angebote technisch nicht gleichwertig ist.**

Dasselbe Prinzip ist anwendbar. Die Standardvertragsklauseln müssen um technische und organisatorische Maßnahmen ergänzt werden, z.B. durch Pseudonymisierungs- und Verschlüsselungsmaßnahmen. Wird das nicht angeboten, muss auf eine europäische Alternative ausgewichen werden.

Anmerkung: Je stärker europäische Alternativen nachgefragt werden, desto größer ist der Markt und desto besser üblicherweise auch das Angebot.

39. **Wie beurteilen sie die Verwendung von AmazonWebServices als CloudService um Webseiten zu hosten.**

AWS hat selbst Datenschutzinformationen herausgegeben. Ob die Maßnahmen hinsichtlich der Vertraulichkeit der Daten ausreichend sind, ist derzeit noch nicht Gegenstand eines veröffentlichten Verfahrens vor einer Aufsichtsbehörde gewesen.

40. **Wie sieht es mit Office 365 aus?**

Office 365 wird prinzipiell mit einer Datenspeicherung in Europa angeboten. Microsoft setzt Maßnahmen, um Zugriff von US-Behörde aufgrund des Cloud-Acts zu beschränken. Ob diese ausreichend sind, ist derzeit noch nicht Gegenstand eines veröffentlichten Verfahrens vor einer Aufsichtsbehörde gewesen.

41. **Bin ich als Agentur dafür verantwortlich/haftbar, wenn datenschutztechnisch nicht alles an der Website korrekt ist?**

Als Agentur müssen Sie Ihrer Warnpflicht als Sachverständige nachkommen, d.h. schriftlich (z.B. per Mail) darüber informieren, dass aus Ihrer Sicht z.B. noch ein IT-Experte oder Anwalt hinzuzuziehen ist. Wenn dies erfüllt ist und der Kunden entscheidet sich für eine nicht-konforme Nutzung der Website, ist dieser auch haftbar und verantwortlich.

42. **Was ist der Unterschied zwischen Anonymisierung und Pseudonymisierung?**

Anonymisierung bedeutet, dass der Personenbezog eines Datums komplett weggenommen wird. Die Daten sind nicht mehr auf eine spezifische Person rückführbar. Pseudonymisierung bedeutet die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

43. **Wie sehr sind davon CDNs betroffen?**

Content Delivery Networks können genauso betroffen sein, daher ist zu prüfen, ob ein Internationaler Datenverkehr in ein unsicheres Drittland stattfindet und müssen entsprechende

Maßnahmen durchgeführt werden (z.B. angemessene technische und organisatorische Maßnahmen).

44. Können CDNs (Content Delivery Networks) als notwendig angesehen werden, oder wären diese ebenfalls innerhalb der Problematik?

Diese sind nach Expertensicht als technisch notwendig anzusehen, ändert aber nichts daran, dass der internationale Datenverkehr in ein sicheres Drittland separat zu prüfen sind, d.h. es müssen dennoch geeignete Maßnahmen (technischer / organisatorischer Art) eingeführt werden.

45. Werden auch „kleine" Websites abgemahnt werden? Wird generell von der Behörde abgemahnt werden oder nur wenn es Kläger gibt?

Die österreichische Datenschutzbehörde kann auf Beschwerde einer betroffenen Person hin oder von Amts wegen tätig werden (ohne Beschwerde von sich aus). Es gibt keine Beschränkung auf „große" Websites oder „große" Anbieter. Jeder, der Tracking mit internationalem Datenverkehr im Einsatz hat, kann hier betroffen sein.

46. Wenn ich Fremdinhalte via iFrame auf meiner Seite einbette, bin ich als Websitebetreiber für dieses Tracking verantwortlich?

Ja, wenn der Betreiber Inhalte einbettet, ist er auch für den dadurch technisch verursachten Datenaustausch verantwortlich. Dies ist von einer allfälligen urheberrechtlichen Verantwortlichkeit zu unterscheiden.

47. Was tut man, wenn man seine Website mit einem Baukastensystem gebaut hat?

Prüfen, was an Trackingmaßnahmen eingesetzt wird, ob ein Datentransfer in die USA z.B. stattfindet. Wenn ja, prüfen, ob man diese Tools durch europäische Anbieter ersetzen kann.

48. Wie sieht es mit Shopify aus?

Shopify ist nach eigenen Angaben eine cloudbasierte Plattform, bei welcher Handelsgeschäfte möglich sind. Ob der Datentransfer problematisch ist, richtet sich nach dem Serverstandort der Cloud, das müsste eruiert werden.

49. Auch auf Tochterunternehmern von US-Unternehmen haben US-Behörden Zugriff?

Richtig. Durch den Cloud-Act ist ein Zugriff der US-Behörden auch auf Niederlassungen in anderen Staaten außerhalb der USA möglich.

50. Gelten diese Regelungen auch für Apps?

Ja, die Regelungen sind technologieneutral und daher auch für mobile Applikationen gleichermaßen wie für Websites anwendbar.