



DSGVO FAQs für Analytics & Digital Marketing

Inkl. DSP, DMP, Adserver, facebook & Programmatic Marketing

Stand: 30.5.2018

Die jeweils aktuelle Version finden Sie unter: www.e-dialog.at/dsgvo-faqs

Einleitung & Management Summary

Wir haben die wichtigsten und drängendsten Fragen aus unseren Enterprise Projekten für Sie hier zusammengetragen. Vorab eine Management Summary, dahinter ausführlich im Detail:

Kurz: Was ist zu tun?

Verträge: Data Ownership & Auftragsverarbeitungsvertrag

Stellen Sie sicher, dass Sie für alle a) Tools und b) Dienstleister Auftragsverarbeitungsverträge bzw. Dienstleistungsvereinbarungen abgeschlossen haben.

Bei Tools sollten Sie darüber hinaus auf Data Ownership achten, das ist nicht automatisch im Auftragsverarbeitungsvertrag enthalten - bei Agentur-Tools gehören die Daten der Agentur.

Informationspflicht

Stellen Sie sicher, dass Sie Ihre User über Art, Umfang und Zweck der Datenerfassung aufklären → Datenschutzerklärung.

Zustimmung - User Consent

Holen Sie die Zustimmung der User zur Erfassung ihrer Daten ein und verwalten Sie diese nachvollziehbar!

1. Es gibt Ausnahmen.
2. Die alte "wir verwenden Cookies und Sie stimmen automatisch zu" Box gilt nicht mehr!

Überprüfung und Dokumentation

Dokumentieren Sie alle verwendeten Systeme, schätzen Sie Risiken ein und erstellen Sie Notfallpläne.

Sichern Sie sich ab, indem Sie die Erfassung von Daten überprüfen lassen, also etwa dass nicht irrtümlich personenbezogene Daten erfasst werden (siehe [Analytics Audit](#)).

Disclaimer

Diese Information stellt keine Rechtsberatung dar, sie ersetzt auch keine individuelle Analyse Ihrer Situation und daher können wir auch keine Haftung übernehmen. Sprechen Sie uns für individuelle Unterstützung gerne an!

Inhalt

Einleitung & Management Summary	2
Kurz: Was ist zu tun?	2
Verträge: Data Ownership & Auftragsverarbeitungsvertrag	2
Informationspflicht	2
Zustimmung - User Consent	2
Überprüfung und Dokumentation	2
Disclaimer	2
Inhalt	3
Teil I: Grundsätzliche Anforderungen	5
Haben Sie Data Ownership & Auftragsverarbeitungsverträge?	5
Brauche ich für jede Agentur einen Vertrag?	5
Wann darf ich Daten nutzen?	5
Haben Sie die Zustimmung der User?	5
User Consent Management im Web	6
User Consent Management Offline (CRM, ...)	6
Informationspflichten	6
Doku-Pflicht, Überprüfung und Risiko-Abschätzung	6
Brauche ich einen Datenschutzbeauftragten?	6
Teil II: Informationen zu Tools	8
Braucht man für Webanalyse eine Zustimmung?	8
Analytics 360, Optimize 360	8
Vertrag / Lizenz & Data Ownership	8
Implementierung / Audit	8
Analytics free, Optimize free	9
Google Analytics: Data Retention Controls	9
Google Analytics: User Löschen / User Deletion API	10
Siehe unseren ausführlichen Artikel zum Löschen von Userdaten in Google Analytics.	10
DoubleClick Suite (DCM, DBM, DS, DRM)	10
DMP	10
Adserver und DSP der Agentur	11
AdWords	11
facebook	11
Tag Management - GTM	11
E-Mail Marketing	11
Sonstige Systeme	12
Was, wenn Systeme verknüpft werden?	12
Customer Match - Upload eigener Kundendaten zu facebook, Google & Co	12
Teil III: konkrete Fragen aus der Praxis	13
Wie kann ich Remarketing DSGVO konform einsetzen?	13

Wie geht Google/DoubleClick mit personenbezogenen Daten um?	13
Was passiert, wenn man als Werbetreibender bis 25.5.2018 die Zustimmung in den Accounts nicht gibt?	13
Wo werden Google Analytics / Google Optimize / Google Suite / Google Tag Manager Daten gespeichert?	13
Google BigQuery Daten in Europa hosten	14
Muss beim Einbau von Pixeln zusätzlich ein Paragraph in die Datenschutzerklärung?	14
Was muss für die neue EU-Datenschutzgrundverordnung beachtet werden?	14
Wie wird e-dialog seine Kunden schad- und klaglos halten?	14
Wieviel Technik-Ressourcen müssen wir einplanen, damit wir mit unseren Systemen aligned sind?	14
Wie gehe ich mit Auskunfts-/Löschanträgen um?	15
Müssen wir alle vor 25.5.2018 ohne User Consent gesammelten Daten löschen?	15
Was muss ich bei Implementierung neuer Features oder Tools beachten?	15
Welche Best-Practice Empfehlungen haben Sie zum sauberen Umgang mit der DSGVO?	16
Zum Abschluss	17
Wie unterstützt uns e-dialog in Bezug auf die DSGVO?	17

Teil I: Grundsätzliche Anforderungen

Haben Sie Data Ownership & Auftragsverarbeitungsverträge?

Die wichtigste Frage ist: Haben Sie für alle von Ihnen oder FÜR SIE genutzten Systeme auch tatsächlich Hoheit über Ihre Daten - **Data Ownership**?

Hier herrscht großer Aufklärungsbedarf - selbst große Unternehmen nutzen Systeme (z.B. Adserver ihrer Agenturen), bei denen die Datenhoheit bei der Agentur verbleibt - beispielsweise dürfen Agenturen DoubleClick-Lizenzen NICHT vererben, [siehe dazu unten im Detail](#).

Wenn Sie alte (= länger bestehende) Lizenzverträge haben (und darin Data Ownership klipp und klar garantiert ist!), sorgen Sie dafür, dass Sie mit jedem Dienstleister und Anbieter auch einen **Auftragsverarbeitungsvertrag** bzw. eine **Dienstleistungsvereinbarung** haben.

Brauche ich für jede Agentur einen Vertrag?

Ja, sofern diese mit Ihren Daten arbeitet - also im Zweifelsfalls: ja.

Diese sollten Sie dokumentieren und in einem Verzeichnis auflisten, dem sogenannten **Verfahrensverzeichnis**.

Für e-dialog Kunden:

Alle unsere Kunden bekommen demnächst einen Auftragsverarbeitungsvertrag / Dienstleistungsvereinbarung. Unsere Analytics 360 und DoubleClick Lizenz-Kunden bekommen im Rahmen ihres Vertrages ein Update dazu.

Wann darf ich Daten nutzen?

Die Nutzung von personenbezogenen Daten ist dann erlaubt, wenn per individuellem User

- a) eine **Einwilligung** (Consent) vorliegt,
- b) es eine **gesetzliche Grundlage** gibt (z.B. zur Erfüllung Ihrer gesetzlichen Aufgaben), oder
- c) **berechtigtes Interesse** vorliegt (wie dieser Punkt ausgelegt wird, ist noch offen, es fehlen Präzedenzfälle)

Am besten abgesichert sind Sie, wenn Sie jedenfalls eine Zustimmung einholen und entsprechend dokumentieren können:

Haben Sie die Zustimmung der User?

Die **Zustimmung** der User muss **ausdrücklich** erfolgen, d.h. die bisherige Praxis des “implied consent” gilt **nicht mehr!** (Bsp: “Durch Nutzung unserer Website stimmen Sie unseren Datenschutzbedingungen zu”, oder “Wir verwenden Cookies...”. Auch “Klicken Sie auf OK um unseren Datenschutzvereinbarung zuzustimmen” gilt nicht, da der User keine Chance hat, abzulehnen.)

Da laut DSGVO das “informierte, freiwillige und explizite Einverständnis der Betroffenen” eingeholt werden muss, sehen wir kaum eine andere Chance für Unternehmen, als dies mit einem Consent Management System zu verwalten:

User Consent Management im Web

- holt aktiv die Zustimmung ein
- verwaltet diese (ermöglicht Änderung der Einstellungen)
- stellt sie allen betroffenen Systemen zur Verfügung (Analytics, Ad-Tech, E-Mail, ...)
- dokumentiert diese (für Anfragen oder juristischen Nachweis)

Bitte “bauen” Sie nicht selbst solche Systeme und überlegen Sie, ob einfache Plugins Ihre Anforderungen erfüllen (siehe oben und das Strafausmaß).

Advanced Systeme können dies auch über Device-Grenzen (Mobile, Desktop, ...) sowie kanalübergreifend (Cookie- sowie E-Mail Opt-In) verwalten.

Gerne unterstützen wir Sie bei der Auswahl, Einführung und des Betriebs Ihres Consent Management Systems. Hier finden Sie [Details](#) bzw. fragen Sie gerne direkt an: kontakt@e-dialog.at

User Consent Management Offline (CRM, ...)

Der Vollständigkeit halber: Natürlich müssen Sie in allen Kanälen und Systemen, bei denen Sie Userdaten digital erfassen, auch eine entsprechende Zustimmung einholen, dokumentieren und verwalten.

Informationspflichten

Gegenüber Ihrer User haben Sie auch Informationspflichten, welche Daten Sie zu welchem Zweck über sie sammeln.

Wie wir das machen, können Sie in unserer [Datenschutzerklärung](#) nachlesen. Disclaimer: Diese dient nur als Beispiel, ist keineswegs perfekt und dieser Link stellt keine Empfehlung oder Beratung dar.

Doku-Pflicht, Überprüfung und Risiko-Abschätzung

Die DSGVO verpflichtet Unternehmen zur Führung eines sogenannten **Verfahrensverzeichnisses**, in dem letztlich alle von Ihnen genutzten Systeme zu dokumentieren sind. Dazu gehört auch die Definition der Art und Qualität der Daten (Datenkategorien), eine **Risiko** (Impact) **Abschätzung** sowie die Erstellung eines **Maßnahmenplans**, sollte es zu einer **Panne** kommen.

Deshalb bieten wir zu Ihrer Unterstützung unser [Google Analytics Audit](#) sowie die [Überprüfung von Data Ownership Ihrer AdServer und DMP Lizenzen](#) an. Damit erfüllen Sie einen wichtigen Teil der DSGVO Anforderungen.

Brauche ich einen Datenschutzbeauftragten?

Nach den kommenden Bestimmungen ist ein Datenschutzbeauftragter jedenfalls von Behörden zu bestellen

sowie bei regelmäßiger Verarbeitung von "besonders schutzwürdigen" personenbezogenen Daten. Diese umfassen Daten aus dem Gesundheitsbereich (inklusive Kennzahlen, wie etwa der Sozialversicherungsnummer) und dem Sexualleben, aber auch politische und religiöse Weltanschauung und etwa Gewerkschaftszugehörigkeit.

Laut derzeitiger Interpretation ist es in Österreich nur dann erforderlich, wenn diese Verarbeitungstätigkeiten den Kernbereich der Geschäftstätigkeit darstellen. Ob diese Ansicht zutreffend ist, ist allerdings noch in Diskussion. Es gibt derzeit keine Liste oder Unterlage der Datenschutzbehörde, die eindeutigen Aufschluss gibt.

Klar ist, dass im Zuge der Gestaltung der Prozesse zu den Betroffenenrechten (Auskunft/Berichtigung/Löschung sowie Verständigung im Falle eines Datenverlustes) in den relevanten Prozessen auch die dementsprechenden Rollen angelegt sein müssen. Hinweis: Nachvollziehbare Prozesse mindern im Schadensfall die Höhe einer eventuellen Strafe.

Sinnvoll und erforderlich ist daher die Bestimmung einer oder eines "**Datenschutz-Verantwortlichen**", um als Koordinationsstelle für Kunden, Lieferanten, Mitarbeiter und - falls erforderlich - der Behörde zu agieren.

Teil II: Informationen zu Tools

Bei allen folgenden Kapiteln und Systemen gilt es, darüber hinaus die Informationspflicht einzuhalten sowie die Zustimmung des Users (einzeln je User und System) einzuholen (sofern kein "berechtigtes Interesse" vorliegt), wie im vorigen Abschnitt beschrieben.

Braucht man für Webanalyse eine Zustimmung?

Wir haben zu Beginn festgestellt, dass wir eine Zustimmung des Users brauchen, WENN kein "berechtigtes Interesse" vorliegt. Im aktuellen Diskurs (April 2018) gehen die meisten Experten davon aus, dass wir die reine Webanalyse keine Zustimmung brauchen, denn im Erwägungsgrund 50 zur DSGVO steht:

„Die Weiterverarbeitung (...) für statistische Zwecke sollte als vereinbarer und rechtmäßiger Verarbeitungsvorgang gelten.“

Gleichzeitig ändert sich die Daten- und Verarbeitungsqualität, sobald Segmentierungen zum Zwecke des Targetings vorgenommen und genutzt werden. Ein Beispiel dafür wäre die Nutzung der Remarketing-Features von Google Analytics in Kombination mit AdWords/GDN oder DoubleClick. Es gibt auch Stimmen, die Remarketing als unternehmerischen Zweck mit berechtigtem Interesse sehen. Vorsichtigerweise könnte man reine Webanalyse ohne Consent nutzen - aber für die Nutzung des Remarketing-Features die Zustimmung einholen.

Analytics 360, Optimize 360

Vertrag / Lizenz & Data Ownership

Für die Enterprise Lizenzen der Analytics 360 Suite von Google stehen seit kurzem neue Auftragsverarbeitungsverträge zur Verfügung, die Sie von Ihrem Reseller bekommen. Sie sind damit vertraglich DSGVO-konform. Darüber hinaus entscheidet die Art der Implementierung, ob Sie das Tool auch DSGVO-konform nutzen, siehe dazu [Implementierung / Audit](#).

Diese Verträge werden einmalig mit dem Lizenznehmer (normalerweise der Konzernmutter/Holding) abgeschlossen - nicht mit den einzelnen Sub-Unternehmen, die eine gemeinsame Analytics-Lizenz nutzen. Dies ist Konzern-intern abzuwickeln.

Wichtig: Die alten (mit Google direkt abgeschlossenen) Auftragsdatenverarbeitungsverträge ersetzen dies nicht - Sie brauchen einen neuen Vertrag!

Achtung: Google hat im April 2018 unglücklicherweise an ALLE Besitzer eines Analytics Accounts die Einladung zum Akzeptieren der Terms im User Interface versendet. Dies GILT NICHT für GA360 Konten und Nutzer.

Implementierung / Audit

Neben dem grundsätzlichen Tool-Vertrag ist noch zu gewährleisten, dass (vor allem irrtümlich) keine personenbezogenen Daten in Ihren Analytics Account einfließen. Dies kann beispielsweise durch falsche

URL-Parameter (etwa aus Formularen, E-Mails u.v.m.) entstehen, auch Events und andere Anpassungen sind häufige Fehlerquellen.

Zur Sicherstellung der DSGVO-konformen Nutzung ihres Analytics Accounts bieten wir ein [Analytics Audit](#) an, in dem wir alle mögliche Fehlerquellen überprüfen, Mängel aufdecken und Empfehlungen zur Bereinigung geben.

→ **Dieses Audit dient als Protokoll zur durch die DSGVO vorgeschriebenen Dokumentation und Risikoeinschätzung.**

Analytics free, Optimize free

Im April 2018 hat Google an alle Besitzer von Analytics-Konten die Einladung zum Akzeptieren des Auftragsverarbeitungsvertrags ausgesendet. Die Einsichtnahme und Zustimmung erfolgt unter "> Verwaltung > Kontoeinstellungen > Zusatz zur Datenverarbeitung".

Wichtig: Die alten (mit Google direkt abgeschlossenen) Auftragsdatenverarbeitungsverträge ersetzen dies nicht - Sie brauchen einen neuen Vertrag!

Google Analytics: Data Retention Controls

Worum geht es?

Sie können jetzt bestimmen, wie lange auf den User bezogene Event Daten in Analytics gespeichert werden.

Welche Daten betrifft das?

Die meisten standardmäßigen Analytics-Berichte basieren auf aggregierten Daten und sind daher nicht betroffen (siehe Beispiel nach Absatz "User Deletion API").

Was sollten Sie wissen?

Google Analytics Free ist standardmäßig auf 26 Monate Aufbewahrungsdauer festgelegt. Bei Analytics 360 ist keine begrenzte Aufbewahrungsdauer voreingestellt.

Alle Eigenschaften haben die gleichen Optionen (14, 26, 38, 50 Monate und "Nicht automatisch ablaufen").

Diese Einstellung gilt zusätzlich zu anderen Methoden der Datenlöschung (d. h. Löschung nach Kontokündigung, PII-Löschungsanforderungen und die neue User Deletion-API).

Die Data Retention Controls bieten die Option die Aufbewahrungsdauer bei neuer Aktivität zurückzusetzen. Exemplarisch bedeutet das:

Wenn die Datenspeicherung beispielsweise auf 14 Monate festgelegt ist, ein Nutzer jedoch jeden Monat eine neue Sitzung initiiert, wird seine Nutzerkennung jeden Monat aktualisiert und erreicht nie den Ablauf von 14 Monaten. Initiiert der Nutzer vor Ablauf der Aufbewahrungsdauer keine neue Sitzung, werden seine Daten gelöscht.

Die Einstellung für die Aufbewahrungsdauer wird von Google noch der [Management API](#) hinzugefügt um die Verwaltung vieler Properties zu erleichtern.

Google Analytics: User Löschen / User Deletion API

Worum geht es?

Die User Deletion API wird die Löschung von auf User bezogenen Daten ermöglichen
Eine neue API, mit der Kunden ihre Daten bei Bedarf löschen können.

Was sollten Sie wissen?

- Ermöglicht das Löschen aller Daten, die mit einem einzelnen Benutzer verknüpft sind, basierend auf Benutzer-ID, Client-ID oder App-Instanz-ID.
- Bis zum 25. Mai verfügbar für Analytics Free als auch für Analytics 360.
- Löschanforderungen werden auf Property-Ebene verarbeitet, d.h. die Löschung erfolgt in allen Datenansichten
- Entfernt alle mit dem Benutzer verknüpften Verlaufsdaten, verhindert jedoch nicht das zukünftige Tracking dieses Benutzers. Eine erneutes Anfordern des Löschens ist möglich.
- Betrifft nicht die Berichterstattung, die auf aggregierten Daten basiert.

Beispiel aggregierte Daten:

Wird ein User-Eintrag mit € 1.000,- Umsatz gelöscht, bleibt die Summe des Umsatzes als aggregierter Wert unverändert. Erst wenn auf den gelöschten User bezogen Daten mit dem Umsatz assoziiert werden sollen, ist das nicht mehr möglich.

Das heisst die Löschung von auf User bezogenen Daten hat generell keine Auswirkung auf die Reports in Google Analytics, da diese auf aggregierten Daten basieren.

Siehe unseren ausführlichen Artikel zum [Löschen von Userdaten in Google Analytics](#).

DoubleClick Suite (DCM, DBM, DS, DRM)

Sofern Sie eine eigene Lizenz mit Vertrag(!) für DoubleClick entweder direkt mit Google oder einem Reseller wie e-dialog haben, bekommen Sie ein Update mit Auftragsverarbeitungsvertrag, englisch DPA - Data Processing Agreement.

Anmerkung für e-dialog Kunden: Die Aufforderung im Interface, die Data Processing Terms akzeptieren zu müssen, können Sie getrost ignorieren, da der Auftragsverarbeitungsvertrag direkt mit uns geschlossen wird.

Achtung: Sollten Sie eine Agentur-Lizenz z.B. Ihrer Media- oder Performance-Agentur mitnutzen, haben Sie keine Data Ownership! Gerne bieten wir Ihnen eine eigene Lizenz mit voller Data Ownership an - das operative Kampagnenmanagement kann dabei wie gewohnt bei Ihrer Agentur bleiben!

DMP

Für Ihre DMP (Data Management Plattform) gilt gleichermaßen: haben Sie einen eigenen Vertrag mit dem Anbieter, der Ihre Data Ownership garantiert sowie einen Auftragsverarbeitungsvertrag enthält, sind Sie auf der sicheren Seite.

Adserver und DSP der Agentur

Sofern Sie für von Ihrer Agentur abgewickelte Kampagnen deren Adserver und DSP (Demand Side Platform, zur Abwicklung von Display-Kampagnen via RTB und Programmatic Buying) nutzen, haben Sie keine Data Ownership! (Eventuell haben Sie zumindest einen Auftragsverarbeitungsvertrag...)

Unser Tipp: Gehen Sie nicht nur im Rahmen der DSGVO auf Nummer Sicher, sondern sichern Sie sich das wertvollste Gut der Zukunft: IHRE DATEN!

Gerne unterstützen wir Sie bei der Überprüfung und Klärung Ihrer Data Ownership und Lizenzverträge! Kontaktieren Sie uns dazu gerne unter kontakt@e-dialog.at oder informieren Sie sich hier über unser [Beratungsangebot](#).

AdWords

Im AdWords Konto unter "Einrichtung >> Einstellungen" sind die "Google-Programm - Bedingungen für Werbetreibende" hinterlegt, denen Sie zustimmen müssen. (Sofern das noch nicht geschehen ist, fordert Google Sie ohnedies durch ein Popup auf.) Darin ist Ihr Auftragsverarbeitervertrag enthalten.

facebook

Bei facebook sind die Informationen für Unternehmen auf folgender Seite zu finden: <https://www.facebook.com/business/gdpr> Dort wird unter anderem erklärt, wann facebook Datenverantwortlicher oder Auftragsverarbeiter ist. Wenn facebook der Datenverantwortliche ist, verarbeiten Sie personenbezogene Daten gemäß den [facebook Datenrichtlinien](#).

Tag Management - GTM

Der Google Tag Manager speichert und überträgt selbst keine Daten. Richtigerweise kann man argumentieren, dass er, obwohl er im Browser des Users abläuft, dort Daten "verarbeitet". Allerdings:

Damit wir überhaupt die Zustimmung des Users einholen, verwalten, würdigen und nachweisen können, ist bei unserer Consent Management Lösung der GTM nötig - es liegt daher jedenfalls "berechtigtes Interesse" vor.

Achtung: Andere Tag Management-Systeme bieten teilweise auch Features an, bei denen sie selbst auch Daten sammeln, verarbeiten und speichern. Dann gilt es wie bei allen anderen Systemen auch, die Data Ownership sicherzustellen sowie Auftragsverarbeitungsverträge zu klären!

E-Mail Marketing

Prüfen Sie Data Ownership sowie Auftragsverarbeitungsvertrag.

Sonstige Systeme

Alles bisher Aufgezeigte gilt für alle Ihre Systeme, die mit Kundendaten arbeiten - dazu gehört jetzt auch schon eine vormals pseudonyme Session-ID!

Prüfen Sie daher Ihr/e

- Web-Formulare,
- Foren- und Chat-Software,
- Shopsystem,
- Zahlungsanbieter
- Werbedienstleister wie Criteo
- etc.

Was, wenn Systeme verknüpft werden?

Die große Stärke von modernem Digital Marketing besteht ja darin, dass User Kanal- und Device-übergreifend in ihrer Customer Journey begleitet und immer zum richtigen Zeitpunkt im richtigen Medium mit der richtigen Botschaft angesprochen werden (= Definition [Programmatic Marketing](#)).

Dabei ist die Herausforderung, den User in möglichst allen genutzten Kanälen und den sie steuernden Systemen zu identifizieren und den User-Status zu synchronisieren.

Kanäle sind etwa Search, facebook, RTB Video/Display/Native, E-Mail, CRM u.v.m.

Systeme sind etwa AdWords, fb Ads, DSP, DMP, Analytics, CRM, DWH u.v.m.

Bei übergreifender Nutzung dieser Systeme sind obige Pflichten einzuhalten, d.h. Informationspflicht und Einholung der Zustimmung.

Auch hier stellt sich wieder die Frage: Haben Sie neben einem Auftragsverarbeitungsvertrag auch Data Ownership in allen beteiligten Systemen?

Customer Match - Upload eigener Kundendaten zu facebook, Google & Co

Customer Match ist ein sehr effizientes Feature, um Kundengruppen aus eigenen Systemen wie bspw. CRM, E-Mail Marketing u.v.m. segmentiert in Werbenetzwerken wie Google, facebook und anderen hochzuladen, um dort genau diese User in Targeting-Audiences optimal ansprechen zu können. Der Schlüssel zur Wiedererkennung der eigenen Kunden ist in der Regel die E-Mail Adresse oder eine Telefonnummer.

Um dies datenschutzkonform bewerkstelligen zu können, bieten alle namhaften Anbieter an, die Schlüssel vorher mit einem Hash-Verfahren zu verschlüsseln, sodass keine Rückschlüsse mehr gezogen werden können. Warum dies die Anforderungen erfüllt und wie dies im Detail geht, erklärt unser ausführlicher Blogartikel [Datenschutz bei Customer Match Listen](#).

Teil III: konkrete Fragen aus der Praxis

Wie kann ich Remarketing DSGVO konform einsetzen?

Wichtig ist, dass ab Mai eine explizite, zweckgebundene Zustimmung des Nutzers für alle Maßnahmen (also auch für Remarketing) wichtig ist. Diese Zustimmung muss für die User auch jederzeit einseh- und änderbar sein. Hilfe dabei leistet ein Consent Management Tool. Darüber hinaus besteht natürlich die Informationspflicht.

Wie geht Google/DoubleClick mit personenbezogenen Daten um?

Google hat sich intensiv mit den Anforderungen der kommenden Datenschutzgrundverordnung (DSGVO) beschäftigt. Etwa 200 Personen (1/3 Anwälte, 2/3 Techniker) haben sich 2 Jahre lang damit auseinandergesetzt, wie deren Geschäftsmodell unter den veränderten Anforderungen funktionieren kann.

Das Resultat ist u.a. ein neuer Dienstleistervertrag, in welchem DoubleClick als Auftragsverarbeiter bestimmte Rechte und Pflichten zugesteht, aber auch die Verantwortung für andere Pflichten klar an den Auftraggeber ("Wer bestimmt welche Daten wie verwendet werden?") abgibt.

Ein guter Ansatzpunkt für den Umgang aus Sicht von Google ist <https://www.google.com/policies/technologies/ads/>, sowie für Advertiser <https://privacy.google.com/businesses/> und für User <https://privacy.google.com/>.

Was passiert, wenn man als Werbetreibender bis 25.5.2018 die Zustimmung in den Accounts nicht gibt?

Google AdWords fordert seit geraumer Zeit seine User in den Werbekonten von Google AdWords und DoubleClick auf, die neuen DPAs - Dataprocessing Agreements zu akzeptieren. Man hat 45 Tage Zeit, die neuen Bestimmungen zu akzeptieren, sonst werden die Kampagnen abgedreht. Ein Start ist erst wieder möglich, wenn man diesen zustimmt.

In **Google DoubleClick** können Sie diese Aufforderung ignorieren, sofern Sie e-dialog Kunde sind; ansonsten wenden Sie sich an Ihren Reseller.

Wo werden Google Analytics / Google Optimize / Google Suite / Google Tag Manager Daten gespeichert?

Google erklärt, dass aufgrund der technischen Bedingungen generell die Verarbeitung von Daten (Speicherung etc.) geografisch nicht eingeschränkt werden kann, gleichzeitig durch den Beitritt in das Privacy Shield alle betroffenen Services einem EU-Unternehmen gleichgestellt sind. Details dazu finden sich hier: <https://privacy.google.com/businesses/compliance/>

Google BigQuery Daten in Europa hosten

Wer die Big Data Engine von Google nutzt, kann die Storage speziell auf europäischen Servern anlegen lassen oder dorthin verschieben. Wie das geht, erklären wir Ihnen gerne im Detail.

Muss beim Einbau von Pixeln zusätzlich ein Paragraph in die Datenschutzerklärung?

Das war auch bisher schon rechtlich eindeutig vorgeschrieben, hier gibt es keine gravierenden Änderungen durch die DSGVO.

Was muss für die neue EU-Datenschutzgrundverordnung beachtet werden?

Es müssen mit Dienstleistern neue Verträge abgeschlossen werden, wenn deren Services benutzt werden sollen. Die Datenschutzerklärung auf der Website wie auch die Einwilligung zur Verwendung von Cookies sollte auch derzeit schon die Verwendung von solchen Systemen widerspiegeln. Mit der DSGVO ändert sich aber auch die potenzielle Strafandrohung, daher ist es ratsam, Angaben und Prozesse nochmals zu überprüfen um unangenehme Überraschungen zu vermeiden.

Relevant werden ggfs. auch die Änderungen durch die ePrivacy-Verordnung, die derzeit in Diskussion ist. Dort werden u.a. die neuen Bedingungen für Cookies verhandelt.

Wie wird e-dialog seine Kunden schad- und klaglos halten?

Prinzipiell ist festzuhalten, dass e-dialog nicht mit personenbezogenen Daten von Betroffenen eines Kunden hantiert. Dies wird u.a. durch die Vorgaben und Einschränkungen von Google und anderen Systemen abgebildet. Weiters unternimmt e-dialog alle notwendigen Schritte - und ein paar mehr als unsere Marktbegleiter -, die technisch und organisatorisch möglich sind um Daten von Kunden am höchstmöglichen technischen Standard abzusichern.

Im Dienstleistungsvertrag mit dem Kunden sind diese abgebildet, wie auch die generellen und speziellen Bedingungen der Auftragsverarbeitung (Hinweispflichten, Fristen etc.).

Wieviel Technik-Ressourcen müssen wir einplanen, damit wir mit unseren Systemen aligned sind?

Grundsätzlich hängen die einzuplanenden Technik-Ressourcen für der Umsetzung der DSGVO davon ab, ob zum Beispiel ein Consent Management System oder eine Eigenlösung zur Anwendung kommt.

Sofern Sie den GTM - Google Tag Manager - im Einsatz haben, können wir die Einführung eines Consent Management Systems für Sie übernehmen und alle Systeme, die über den GTM eingebunden werden

berücksichtigen. Der Aufwand dafür ist Ihrerseits nahezu Null und bei uns in einem Standardprozess abgedeckt. (Und sollten Sie noch keinen GTM im Einsatz haben, wäre das nun wirklich der entscheidende Anstoß!)

Im Falle einer Eigenlösung hängen die einzuplanenden Ressourcen an der spezifisch geplanten Umsetzung, der Anzahl der Systeme und beteiligten Personen und Firmen.

Wie gehe ich mit Auskunfts-/Löschanträgen um?

Die Rechte der Betroffenen auf Auskunft, Richtigstellung, Einschränkung der Datenverarbeitung und Löschung unterscheiden sich in der Datenschutzgrundverordnung wesentlich nur in einem Punkt von den bisherigen Bestimmungen: Die Frist zur Beantwortung wird von 8 Wochen auf 4 Wochen verkürzt. Daher sollen die internen Prozesse, wie etwa ein Auskunftsbegehren beantwortet wird, vorher festgelegt werden und auch die entsprechenden Rollen (z.B. Datenschutzbeauftragter, "Datenschutzverantwortlicher") eingeplant werden.

Verantwortlich für die Bearbeitung ist der Auftraggeber ("Controller") und den Auftragsverarbeiter ("Processor") treffen hier bestimmte Mitwirkungspflichten, etwa die möglichst rasche Weitergabe von bei ihm irrtümlich eingelangten Auskunftsbegehren sowie, wenn zweckmäßig, Mitwirkungspflichten bei der Beantwortung der Auskunft.

Prinzipiell muss jedes Auskunftsbegehren geprüft und beantwortet werden, auch wenn keine zu beauskunftenden Daten verarbeitet werden. Der erste Schritt ist immer die Prüfung, ob diejenige Person, die ein solches Begehren stellt, überhaupt zur Auskunft berechtigt ist. Dieses Begehren muss schriftlich eintreffen, angeschlossen muss eine Kopie eines Lichtbildausweises sein. Brief und Fax sind jedenfalls zulässig, Anfragen per E-Mail werden selten akzeptiert. Empfehlenswert ist es, die Antwort mit einem eingeschriebenen Brief auszufolgen.

Müssen wir alle vor 25.5.2018 ohne User Consent gesammelten Daten löschen?

Oder: **Wie soll mit bestehenden Daten umgegangen werden?**

Da in der Vergangenheit betreffend Erklärung, Zustimmung und Einwilligung keine grundlegend anderen Regeln gegolten hatten, können in vielen Fällen die bisherigen Daten weiterverwendet werden. Es ist dabei auch zu prüfen, ob eine datenschutzrechtliche Einwilligung überhaupt erforderlich ist oder eine andere Rechtsgrundlage herangezogen werden kann.

Was muss ich bei Implementierung neuer Features oder Tools beachten?

Grundsätzlich: Besprechen Sie das mit Ihrem Datenschutzbeauftragten oder Datenschutzverantwortlichen - der (oder die) ist dafür letztlich verantwortlich!

Unser Tipp: Prüfen Sie, ob neue Datenkategorien erfasst werden, dann muss dafür die Information upgedated und die Zustimmung eingeholt werden.

Achtung: Wenn zusätzlicher Consent eingeholt werden muss → holen Sie den ein!

Gegebenenfalls ist dies auch zu berücksichtigen, wenn vorheriger/alter Consent zu schwach ist, d.h. dass dann bestehende Consents neu bzw. aktualisiert eingeholt werden müssen. Dies kann mit einem User Consent Management System recht einfach DSGVO-konform abgebildet werden.

Immer: Testen! Nach jeder Implementierung testen Sie nicht nur die Funktion, sondern auch Missfunktion im Sinne der DSGVO: werden tatsächlich nur die Daten gesammelt, die definiert wurden? Oder werden irrtümlich personenbezogene Daten erfasst? Werden die Consent-Einstellungen der User gewürdigt?

→ Wir unterstützen Sie hierbei gerne mit unseren Audits und laufender Wartung Ihrer Consent Management Lösung.

Welche Best-Practice Empfehlungen haben Sie zum sauberen Umgang mit der DSGVO?

Gehen Sie anhand von Use-Cases vor und beschreiben Sie, was gemacht werden soll, welche Tools mit welchen Datenkategorien zum Einsatz kommen, um was zu bezwecken. Dann gehen Sie mit Ihren Datenschutzverantwortlichen alle Cases durch und entscheiden, welche "safe" sind, für welche noch weitere Bedingungen vor ihrem Einsatz zu erfüllen sind, und welche einfach "no-go" sind...

Schließlich vergessen Sie nicht, alles zu dokumentieren, den User zu informieren, Consent einzuholen, Risiken abzuschätzen und zu dokumentieren und Pläne für einen Notfall je Use-Case zu definieren.

Zum Abschluss

Wie unterstützt uns e-dialog in Bezug auf die DSGVO?

Als Vorreiter in Datadriven Advertising und Digital Analytics beschäftigen wir uns intensiv mit allen nötigen Aspekten der DSGVO und unterstützen Sie gerne in der Umsetzung der nötigen Maßnahmen.

Konkret bieten wir folgende Unterstützung an:

- diese umfassende Information (laufend aktualisiert)
- dass unsere Mitarbeiter geschult und sensibilisiert sind, dass wir intensiv möglich darauf achten, dass sorgsam mit personenbezogene Daten umgegangen wird und der User im Mittelpunkt steht
- [Analytics Audit auf personenbezogene Daten laut DSGVO](#)
- [Prüfung Ihrer Adserver und DMP Lizenzen](#)
- [Einführung und Wartung Ihres User Consent Managements](#)
- [Analyse der Menge an Usern ohne Consent](#)
- Unterstützung bei Auskunfts- und Löschanträgen wie in unserer Dienstleistungsvereinbarung und - bei GA360 und DCLK-Lizenzkunden - dem Auftragsverarbeitungsvertrag definiert
- Klärung aller offenen Fragen aus unserem Kompetenzbereich sowie Umsetzung der vereinbarten Maßnahmen: nach Aufwand

Was wir nicht machen:

- Juristische Beratung
- Wir sind nicht Ihre Datenschutzbeauftragten

Wir hoffen, dass unsere DSGVO-FAQ für Marketer Ihnen eine kleine Unterstützung sein konnte und Sie konform alle Potentiale von erfolgreichem digitalen Marketing ausschöpfen können!

Kontaktieren Sie uns:

Österreich:	www.e-dialog.at	+43 1 309 09 09
Deutschland:	www.e-dialog.de	+49 322 210 93 284
Schweiz:	www.e-dialog.ch	+41 43 508 04 14