WHITEPAPER

etracker®

Orientierungshilfe zur datenschutzgerechten Nutzung von Tracking-Diensten für Websites und Apps

Einleitung

Wir werden regelmäßig gefragt, welche Anforderungen ein Website-Betreiber erfüllen und auf welche Dinge er achten muss, um den neuen Regelungen der Datenschutz-Grundverordnung (DSGVO) beim Tracking von Websites, Apps und Online-Marketing-Maßnahmen gerecht zu werden.

Um den datenschutzkonformen Einsatz von etracker unter DSGVO und BDSG neu zu gewährleisten, haben wir uns mit den Aufsichtsbehörden abgestimmt, die Datenschutz-Zertifizierung mit Verleihung des ePrivacyseal-Gütesiegels durchlaufen und uns mit vielen Datenschutzberatern und Fachanwälten ausgetauscht.

Unser dadurch gewonnenes Fachwissen und unsere praktische Erfahrung in Sachen DSGVO-konformes Tracking möchten wir hier mit Ihnen teilen.

Die häufigsten Fragestellungen, die in den vergangenen Wochen an uns herangetragen wurden, lassen sich in diese sechs Fragen unterteilen, die im Folgenden behandelt werden:

- Wann fällt der Einsatz von Tracking-Diensten nicht unter die DSGVO, da kein Personenbezug besteht?
- Wann ist der Einsatz von Tracking-Diensten einwilligungspflichtig und nicht durch Interessenabwägung gerechtfertigt?
- Wie müssen gesetzeskonforme Einwilligungen gestaltet sein?
- Was sind sonstige Anforderungen an DSGVO-konformes Tracking?
- Was heißt das insgesamt für den Einsatz von Google Analytics & Optimize im Vergleich zu etracker Analytics & Optimiser?

Wann fällt der Einsatz von Tracking-Diensten nicht unter die DSGVO, da kein Personenbezug besteht?

Das Tracking von rein Session-bezogenem Verhalten von Website-Besuchern ist nicht von der DSGVO betroffen, da ein Personenbezug nicht vorliegt. Keinen Personenbezug haben dabei zum Beispiel:

- Seiten-Eigenschaften: Domain, Pfad, Seiten-URL und Titel (bei Sicherstellung, dass darin keine personenbezogenen Daten enthalten sind; Achtung insbesondere bei automatischer Erfassung von URL-Parametern)
- Browsing data: Referrer
- Browser data: Scroll-Tiefe, User Agent
- Interaction data: Event-Name und Eigenschaften (Warenkorb-Events, Audio- und Video-Events, Downloads u.ä.); ausgenommen die Nutzereingaben in Such- und Formularfelder
- Geografische Daten auf Landes-, Regions- und Stadtebene

Diese Daten dürfen sogar dann erfasst werden, wenn Besucher in ihrem Browser „Do Not Track“ (DNT) aktiviert oder in anderer Form der Verarbeitung ihrer personenbezogenen Daten widersprochen haben.

Aber: Dabei ist immer sicherzustellen, dass:

- keine Identifikatoren für Cross Device Tracking verarbeitet werden.
- vollständige IP-Adressen weder gespeichert noch verarbeitet werden.
- keine Bestellnummern erfasst werden.
- ausschließlich Session Cookies eingesetzt werden.
- keine Informationen erfasst werden, mit denen ein bestimmtes Gerät Session-übergreifend identifiziert werden kann, etwa eindeutige Gerätekennungen wie IDFA, UDID, Android-ID oder Google Advertising ID.
- feingranulare geografische Daten wie GPS-Daten, Postleitzahlen oder Längen- und Breitengrade nicht erfasst werden.

Wann ist der Einsatz von Tracking-Diensten einwilligungspflichtig und nicht durch Interessenabwägung gerechtfertigt?

Eine Einwilligung der Betroffenen ist immer dann erforderlich, wenn umfassende Profile - insbesondere über verschiedene Websites hinweg - gebildet, also in großem Stil Verhaltens- und Persönlichkeitsprofile der Betroffenen erstellt werden. Von einem derart intensiven Eingriff in die Privatsphäre und Persönlichkeitsrechte der Betroffenen ist zudem auszugehen, wenn

- Anbieter das Recht auf die Daten beanspruchen und diese nutzen, um ihre eigenen Produkte und Services zu verbessern
- die Daten an Dritte weitergegeben werden oder Werbekunden bzw. Marketingpartner diese direkt oder indirekt nutzen können
- besonders sensible Datenkategorien erhoben werden
- keine Pseudonymisierung bzw. eine ausreichende Verschlüsselung (durch geeignete Hashverfahren) bei der Verarbeitung erfolgt

Beim Einsatz von Google Analytics beispielsweise werden laut der aktuellen Google Datenschutzerklärung Daten über Aktivitäten von Besuchern über mehrere Websites hinweg, die Google Analytics einsetzen, verknüpft.

Google Datenschutzerklärung Stand: 25.05.2018 (Wirksamkeit), recherchiert am 27.06.2018:
„Wenn Sie Websites besuchen, auf denen Google Analytics eingesetzt wird, werden Google und der Google Analytics-Kunde gegebenenfalls Daten über Ihre Aktivitäten auf dieser Website mit Aktivitäten auf anderen Websites verknüpfen, auf denen ebenfalls unsere Werbedienste genutzt werden.“

Hier ist eine Interessenabwägung nicht gerechtfertigt.

Wie müssen gesetzeskonforme Einwilligungen gestaltet sein?

Wenn Einwilligungen erforderlich sind, reichen gewöhnliche Cookie-Hinweise nicht aus. Denn es muss eine aktive Wahlmöglichkeit bestehen und erst nach einer explizit bestätigenden Handlung mit „Ich stimme zu“, „Ich bin einverstanden, dass…“ oder Ähnlichem darf eine Datenerfassung erfolgen.

Eine Einwilligung ist nicht wirksam, wenn diese quasi erzwungen wird, indem etwas ein Einwilligungsdialog nicht ohne Akzeptieren geschlossen werden kann. Eine Nutzung der Website

muss auch ohne Zustimmung einer Datenerfassung möglich sein. Außerdem muss eine differenzierte Zustimmung oder Ablehnung unterschiedlicher Zwecke und Methoden erfolgen können und die Ablehnung darf nicht unnötig schwer gemacht werden, etwa durch ein mühsames Abwählen von einzelnen Diensten aus einer längeren Liste oder das Wechseln auf die Web-Seiten der jeweiligen Anbieter.

Zudem müssen Einwilligungen nachvollziehbar dokumentiert werden – mindestens mit Nachweis von Cookie-ID und Timestamp (Datum und Uhrzeit).

Was sind sonstige Anforderungen an DSGVO-konformes Tracking?

Wenn ein Tracking rechtmäßig auf Basis eines berechtigten Interesses oder einer Einwilligung von Betroffenen stattfindet, ist weiterhin zu beachten:

- Auftragsverarbeitungsvertrag mit Anbieter abschließen
- Beachtung von Do Not Track-Headern (DNT)
- IP-Maskierung vor der eigentlichen Verarbeitung zum frühestmöglichen Zeitpunkt
- Verschlüsselung von Remarketing- und Cross-Device-IDs (SHA256 als Mindestanforderung für Hashing)
- Nur Verarbeitung von pseudonymisierten Daten; keine Verwendung von Klardaten
- Implementierung einer Widerspruchsmöglichkeit (Opt-Out), die ohne Plugin-Installation auskommt (auch mobil bzw. Endgeräte-unabhängig funktioniert) und direkt auf der jeweiligen Website ausgeübt werden kann
- Ausreichende und klare Informationen zur Datenverarbeitung (IDV) im Sinne von Art. 12, 13 DSGVO (Datenschutzerklärung)
- Einhaltung der Kontrollpflichten des Website-Betreibers durch Sachverständigen-Testat bzw. Datenschutz-Audit

Was heißt das insgesamt für den Einsatz von Google Analytics & Optimize im Vergleich zu etracker Analytics & Optimiser?

Google Analytics und Google Optimize können datenschutzkonform nur eingesetzt werden, wenn Website-Betreiber mindestens

- sich selber um die Einholung expliziter, informierter Einwilligungen der Nutzer kümmern (differenzierte Zustimmung zu Web-Analyse und Werbefunktionen).
- einen Auftragsverarbeitungsvertrag mit Google LLC und den Zusatz zur Datenverarbeitung von Analytics mit Google abschließen.
- Verfahren implementieren, so dass DNT-Header berücksichtigt werden.
- die Funktion IP-Maskierung („anonymizeIP“) auf sämtlichen Website-Seiten implementieren, damit das letzte Oktett der IP-Adresse vor jeglicher Speicherung gelöscht wird.
- das Deaktivierungs-Add-On implementieren, mit dem Betroffenen die Möglichkeit zum Widerspruch (Opt-Out) gegen die Erfassung von Nutzungsdaten eingeräumt wird (für alle gängigen Browser und Endgeräte).
- das sog. „Disabling Tracking“ implementieren; ein Opt-Out Cookie, mit dem der User durch einen einfachen Klick das Analytics-Tracking unterbinden kann. Dies ist notwendig, weil das zuvor genannte Deaktivierungs-Add-On auf vielen (mobilen) Endgeräten nicht funktioniert.
- Informationen zur Datenverarbeitung (IDV) im Sinne von Art. 12, 13 DSGVO in der Datenschutzerklärung im Hinblick auf Google-Dienste integrieren (Google liefert keine eigene Vorlage).
- die User-ID nicht aktivieren bzw. deaktivieren.
- die Kontrollpflichten hinsichtlich der Einhaltung der technisch-organisatorischen Maßnahmen erfüllen.

Ein DSGVO-konformes Tracking ist mit etracker Analytics und etracker Optimiser deutlich einfacher sichergestellt, denn:

- die explizite, informierte Einwilligung der Nutzer ist im Regelfall nicht erforderlich. Somit werden deutlich mehr Besucher getrackt.
- der AV-Vertrag mit etracker kann elektronisch abgeschlossen werden.
- DNT-Header werden ab Tracking Code 4.1 automatisch berücksichtigt.
- die IP-Maskierung erfolgt automatisch und erfordert keine spezielle Konfiguration des Tracking Codes.
- die von etracker bereitgestellte Widerspruchsfunktion wird von allen gängigen Browsern und Endgeräten unterstützt.
- etracker bietet eine Vorlage für den Datenschutzhinweis im Sinne von Art. 12, 13 DSGVO in den Account-Einstellungen an.
- es müssen keinerlei Zusatzfunktionen deaktiviert werden oder Ähnliches.
- die Kontrollpflichten werden durch die unabhängige Prüfung und Zertifizierung mit dem ePrivacy-Siegel erfüllt.

Gerne stehen wir für Sie bereit, wenn Sie Fragen zu dieser DSGVO-Orientierungshilfe haben oder mehr darüber erfahren möchten, wie Sie mit etracker das Maximum aus Ihrem wertvollen Datenschatz holen und gleichzeitig die Anforderungen der DSGVO erfüllen sowie die eigene Datenhoheit sichern.

Stand: 09.01.2019