etracker®

Web-Analyse, Konversions-Optimierung und Online-Marketing Steuerung unter EU-DSGVO und BDSG neu

So tracken Sie auch nach dem 25. Mai 2018 rechtskonform weiter

Die „Online-Marketing Klausel“ der EU-DSGVO

Für Online-Marketer ist Art. 6 eine der entscheidenden Passagen in der EU-DSGVO, denn hier geht es um die Rechtmäßigkeit der Verarbeitung personenbezogener Daten.

Art. 6 Abs. 1 der EU-DSGVO besagt, dass die Verarbeitung von personenbezogenen Daten [im Sinne von Tracking (Anmerkung etracker)] nur rechtmäßig ist, wenn:

> lit. a: „Die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben [hat];“
>
> oder
>
> lit. f: „die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich [ist], sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.“

Eine Einwilligung bzw. ein Opt-In ist demnach dann **erforderlich**, wenn bei der Abwägung der Interessen, der Schutz der betroffenen Person überwiegt.

Das ist der Fall, wenn

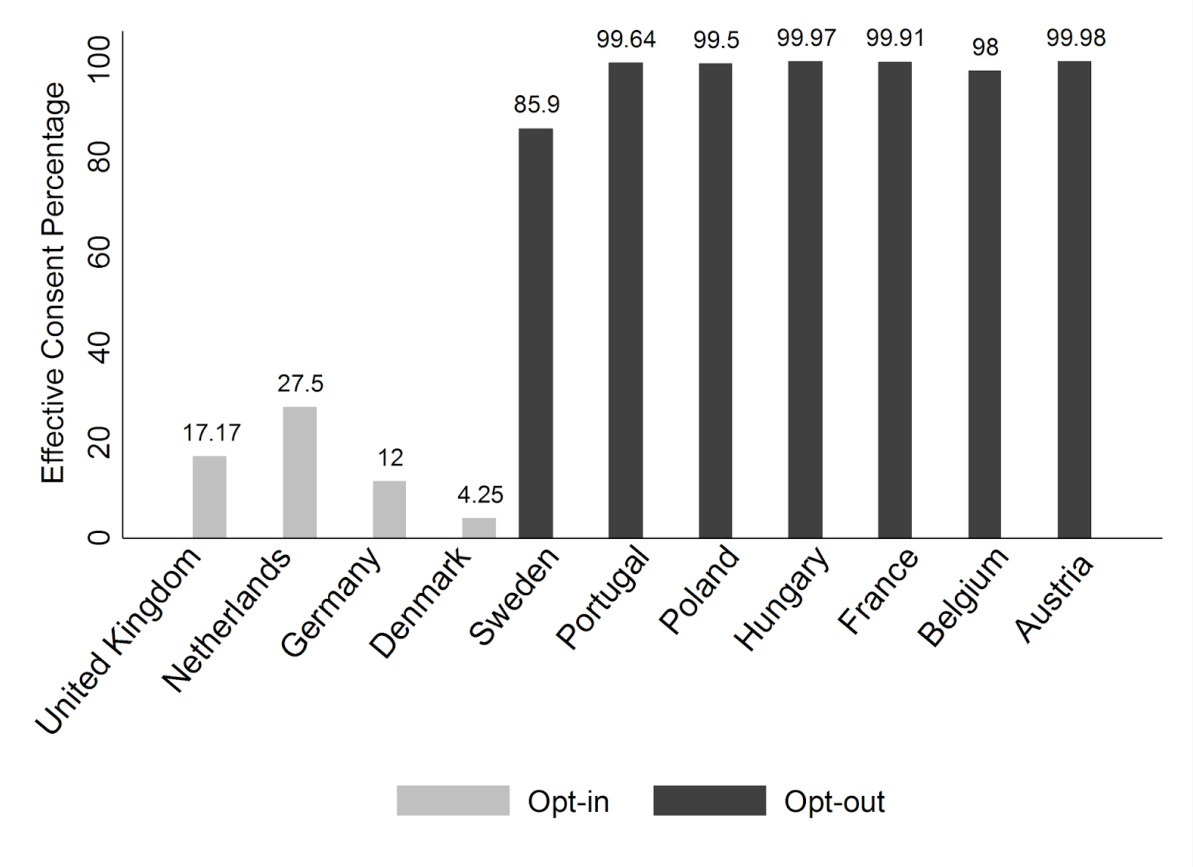
- Anbieter das Recht auf die Daten beanspruchen und diese nutzen, um ihre eigenen Produkte und Services zu verbessern,
- die Daten an Dritte weitergegeben werden,
- Daten von Kindern oder besonders sensible personenbezogene Daten erhoben werden,
- die Daten zu einer übergeordneten Profilbildung genutzt werden,
- keine Pseudonymisierung bzw. ausreichende Verschlüsselung (durch geeignete Hashverfahren) bei der Verarbeitung erfolgt,
- eine Übermittlung in ein Drittland außerhalb der EU erfolgt, ohne die damit einhergehenden zusätzlichen Auflagen zu erfüllen,
- E-Mailings an Nicht-Kunden oder zu „unähnlichen“ Produkten versendet werden.

Keine Einwilligung ist notwendig, **solange**

- der Zweck - wie Direktwerbung, Marktforschung (Web-Analyse und A/B-Testing) oder bedarfsgerechte Gestaltung des Angebots (Personalisierung) - hinreichend klar formuliert ist und real besteht (Zweckbindung),
- Datensparsamkeit, Anonymisierung bzw. Pseudonymisierung und Sicherheitsmaßnahmen beachtet werden,
- keine hochsensiblen Daten verarbeitet werden,
- keine erhebliche Beeinträchtigung oder mögliche Nachteile für Betroffene zu erwarten sind,
- die Verarbeitung üblich und vernünftigerweise von betroffenen Personen abzusehen bzw. zu erwarten ist und
- ein geringes Verbreitungspotenzial der Daten vorliegt.

Warum kommt dem Einwilligungserfordernis (Opt-In versus Opt-Out) eine so große Bedeutung zu?

Ein Blick auf das Ergebnis des Ländervergleiches einer internationalen Studie zum Einverständnis zur Organspende macht es deutlich. Der sogenannte „Default-Effekt“ sorgt für einen gravierenden Unterschied: In den Ländern, in denen man sich über ein Opt-Out aktiv von der Organspende ausschließen muss, liegt die Spenderbereitschaft bei nahezu 100%. Die Länder, in denen man sich über ein Opt-In aktiv für die Organspende melden muss, profitieren nur von einer Spenderbereitschaft von weit weniger als 28%.



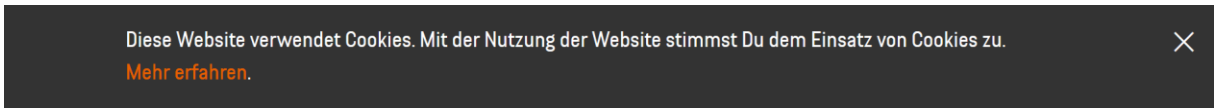
Quelle: The effect of default choices on organ donation. Quelle: Johnson and Goldstein (2003)

Dieses Beispiel zeigt, dass Compliance-Bemühungen nicht nur dazu dienen sollten, die Gefahren von Abmahnungen, Strafen und Bußgelder zu vermeiden, sondern Lösungen eingesetzt werden müssen, die der Compliance entsprechen, jedoch mögliche Compliance-Nachteile minimieren oder gar keine Nachteile mit sich bringen. Denn sobald die eingesetzte Lösung bzw. Art der Datenverarbeitung ein Opt-In erforderlich macht, muss mit einer deutlich geringeren Daten-Erfassungsrate gerechnet werden.

Fazit: Für die Gewährleistung einer bestmöglichen wie rechtskonformen Daten-Erfassungsrate entscheidend:
Alle Arten der Datenverarbeitung sollten nach Möglichkeit durch die Rechtsgrundlage des Art. 6 Abs. 1 f EU-DSGVO zu rechtfertigen sein.

Wenn ein Opt-In erforderlich sein sollte: Wie sieht dann eine rechtskonforme Einwilligung aus?

Heute in der Praxis verbreitete Hinweise wie z. B.:



erfüllen die gesetzlichen Anforderungen an eine EU-DSGVO-konforme Einwilligung nicht!

Denn die Einwilligung muss darüber informieren:

- Welche(s) Verfahren/Produkt(e) kommt(en) zum Einsatz?
- Welche Arten von personenbezogenen Daten werden verarbeitet?
- Für welchen Zweck werden die Daten verarbeitet?
- Hinweis auf Opt-Out-Möglichkeit

Und ganz wichtig: Eine aktive Wahlmöglichkeit muss geboten werden!

Was heißt das für die Nutzung von Google Diensten?

Bei Einsatz der Tracking-Tools von Plattform-Betreibern wie Google und Facebook, die das Recht auf Ihre Daten beanspruchen und diese nutzen, um ihre eigenen Produkte und Services zu verbessern, oder US-Tools, die IP-Adressen und Gerätekennungen nur mangelhaft anonymisieren oder verschlüsseln, laufen Sie Gefahr, eine Einwilligung von Ihren Nutzern zu benötigen.

In der Google Datenschutzerklärung Stand 18.12.2017 (recherchiert am 26.02.2018) heißt es:
„Bei Verwendung von Google Analytics zusammen mit unseren Werbediensten, z. B. solchen, die das DoubleClick-Cookie nutzen, werden Google Analytics-Daten vom Google Analytics-Kunden oder von Google mithilfe von Google-Technologie mit Daten über Besuche auf mehreren Websites verknüpft."

Somit ist klar: Bei Verwendung von Google Analytics zusammen mit Googles Werbediensten erfolgt keine rein zweckgebundene, transparente Auftragsdatenverarbeitung, sondern eine Verarbeitung darüber hinaus für eigene Zwecke.

Es ist zum einen fraglich, ob es sich hierbei um ein berechtigtes Interesse von Dritten gemäß Art. 6 EU-DSGVO handelt, zum anderen könnten sehr wahrscheinlich die „Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen", da eine Website-übergreifende Profilerstellung vorgenommen wird.

Insofern ist davon auszugehen, dass bei Verwendung von Google Analytics zusammen mit Googles Werbediensten eine explizite Einwilligung vor der Verarbeitung durch die betroffenen Personen erforderlich ist. Hierbei sind die Anforderungen an eine EU-DSGVO-konforme Einwilligung zu beachten, insbesondere die Notwendigkeit einer aktiven Zustimmung von Seiten der betroffenen Personen.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit weist nach einer Prüfung von Google Analytics im Januar 2017 zwar explizit darauf hin, dass die Prüfung der Nutzung von Google Analytics nicht im Zusammenhang mit den Werbe-Diensten von Google erfolgte:

„Eine Bewertung der Datenschutzrechtlichen Zulässigkeit anderer, im Zusammenhang mit Google Analytics angebotenen Marketing-Instrumente und Werbe-Dienste (z.B. AdSense, AdWords oder erweiterte Funktionen von Google Universal Analytics), erfolgte nicht. Sie waren nicht Gegenstand der Prüfung. Die vorstehenden Hinweise treffen damit auch keine Aussage über die datenschutzrechtliche Zulässigkeit des Einsatzes dieser Dienste."
(https://www.datenschutz-hamburg.de/uploads/media/GoogleAnalytics_Hinweise_fuer_Webseitenbetreiber_in_Hamburg_2017.pdf)

Doch auch wenn der Einsatz von Google Analytics von der Hamburgischen Datenschutzbehörde als rechtskonform bewertet wurde, so gilt dies nur unter Beachtung vieler Faktoren, die Sie als Website-Betreiber berücksichtigen und somit Hindernisse, die Sie überwinden müssen. So müssen Sie durch entsprechende Einstellungen im Google Analytics- Programmcode Google mit der Kürzung der IP-Adressen beauftragen. Dazu ist auf jeder Internetseite mit Analytics-Einbindung der Trackingcode um die Funktion „_anonymizeIp()" zu ergänzen, was für Sie zum einen extra Arbeitsschritte bedeutet und zum anderen Risiken in sich birgt, z. B. durch das Vergessen oder Übersehen einer Seite.

Wird Google Analytics ohne Googles Werbedienste eingesetzt, so kann auch dann nicht ausgeschlossen werden, dass eine explizite Einwilligung erforderlich ist. Beispielsweise könnte ein Personenbezug herstellbar werden, wenn die soziodemografischen Daten im Google Analytics-Konto aktiviert werden. Außerdem müsste ausgeschlossen werden, dass Google eine Verknüpfung über mehrere Websites vornimmt oder eine Nutzung der Daten zur Optimierung der eigenen Dienste ausschließt – unabhängig von den entsprechenden Einstellungen, die der Kontoinhaber eigenständig vornehmen kann.

Ihre Daten – Ihre Verantwortung

Bitte beachten Sie, dass Ihnen als Website-Betreiber eine Auswahlverantwortung der von Ihnen genutzten Dienste obliegt. Sie als Verantwortlicher dürfen nur mit Auftragsverarbeitern arbeiten, die gemäß Art. 28 Abs. 1 EU-DSGVO hinreichend garantieren können, dass „geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen" der EU-DSGVO erfolgt und die Rechte der betroffenen Personen geschützt werden.

Die etracker Produkte sind 100% datenschutzkonform gemäß EU-DSGVO und BDSG neu

etracker Analytics und etracker Optimiser wurden in einem umfänglichen technischen wie juristischen Verfahren von unabhängigen Datenschutz-Experten geprüft. Die Einhaltung der Regelungen von EU-DSGVO und BDSG neu wurde bestätigt, zertifiziert und mit dem Datenschutz-Gütesiegel *ePrivacyseal* ausgezeichnet.

Wichtig: Die ePrivacy-Experten halten es für vertretbar, die Datenverarbeitung mit etracker Analytics und Optimiser durch die Rechtsgrundlage des Art. 6 Abs. 1 f EU-DSGVO zu rechtfertigen. Das heißt: Sie als Website-Betreiber benötigen keine explizite Einwilligung zur Auftragsverarbeitung.

Datenschutz genießt bei uns seit jeher höchste Priorität

Zur „etracker DNA" gehört u.a. ein sehr hoher Anspruch an den korrekten und vertraulichen Umgang mit Besucher- und Kundendaten. Als erstem Anbieter von Lösungen zur Analyse und Optimierung von Websites und Online-Marketing Maßnahmen überhaupt, wurde uns bereits 2006 nach einem aufwändigen Prüfverfahren durch den Hamburgischen Datenschutzbeauftragten die datenschutzrechtliche Konformität bescheinigt.

Wir kennen die Datenschutz-Bestimmungen genau und stehen mit den Aufsichtsbehörden im kontinuierlichen Dialog. So haben wir schon frühzeitig die Anforderungen der EU-DSGVO durch Privacy by Design umgesetzt. Um Ihnen die Sicherheit zu geben, mit etracker bereit für die EU-DSGVO zu sein, haben wir uns zudem von den Experten der ePrivacy GmbH prüfen lassen (siehe oben).

Was tut etracker konkret, um die DSGVO-Compliance zu gewährleisten?

✓ Pseudonymisierung und Anonymisierung

Bei der Speicherung der Besucherdaten werden insbesondere auch die IP-Adressen, Geräte- und Domaindaten der Besucher nur verkürzt gespeichert beziehungsweise verschlüsselt, so dass ein Rückschluss auf den einzelnen Besucher nicht möglich ist. Wir verpflichten uns, erhobene Daten niemals mit anderen Datenbeständen zusammenzuführen, z.B. um einen Personenbezug herzustellen.

Die Kürzung der IP-Adresse erfolgt zum frühestmöglichen Zeitpunkt und zwar standardmäßig automatisiert, ohne dass Sie als Kunde spezielle Anpassungen oder Konfigurationen vornehmen müssen. Damit bieten wir Ihnen die geforderten datenschutzfreundlichen Voreinstellungen (Privacy by Design und Privacy by Default).

Identifier zur Wiedererkennung eines App-Nutzers, Durchführung von Session- und Cross-Device-Tracking sowie Bereitstellung von verhaltensbezogenen Daten für Remarketing werden sicher pseudonymisiert bzw. verschlüsselt.

✓ etracker stellt Daten ausschließlich dem jeweiligen Kunden zur Verfügung

Wir verarbeiten Ihre Daten ausschließlich in Ihrem Auftrag gemäß abgeschlossener Auftragsdaten-vereinbarung. Ihre Daten gehören Ihnen und werden nicht mit anderen Daten zusammengeführt oder gar an Dritte weitergegeben. Wir betreiben keinerlei Datenhandel noch nutzen wir Ihre Daten für übergeordnete Analysen oder Profilbildungen.

✓ Verarbeitung und Speicherung in Deutschland

Unser Rechenzentrum ebenso wie die Entwicklung und System-Administration befinden sich in Hamburg, Deutschland. Wir nutzen die hochwertige, hochsichere und hochverfügbare Rechenzentrum-Infrastruktur der ISO/IEC 27001:2013 zertifizierten IPHH Internet Port Hamburg GmbH für sogenanntes Server-Housing ohne externen Zugriff auf Applikationen und Daten.

✓ Optionaler Betrieb im eigenen Rechenzentrum

Für das Tracking hochsensibler Anwendungen und Portale empfehlen wir den Betrieb unserer Lösungen in Ihrem Rechenzentrum oder der von Ihnen genutzten Private Cloud. In unserer On-Premise-Installation sind alle hierfür notwendigen Bausteine enthalten: Code-Auslieferung, Zählungsannahme und Applikation. So kann die Gefahrenabwehr vollständig durch Ihre eigenen Schutzmaßnahmen erfolgen. Keine Kompromisse bei der Sicherheit oder bei der Leistung: Sie profitieren von der hoch performanten Big Data Analytics-Technologie auf Rohdaten-Basis, die genauso im SaaS-Betrieb zum Einsatz kommt.

✓ EU-DSGVO-konforme Vereinbarung zur Auftragsverarbeitung (AV-Vertrag)

Um eine Verarbeitung von Daten im Auftrag datenschutzkonform umzusetzen, ist zunächst ein Vertrag zur Auftragsverarbeitung (AV-Vertrag) gemäß Art. 28 DSGVO zu schließen. Dies kann bei etracker bequem elektronisch erfolgen. Der Vertrag wurde in Anlehnung an die Vorlagen von deutschen Landesdatenschutz-Ämtern von einer auf IT-Recht und Datenschutz spezialisierten Anwaltskanzlei auf die Belange der etracker Web-Analyse und Konversionsoptimierung angepasst.

✓ Datenschutzhinweis, Einwilligung und Widerspruchsmöglichkeit auf Ihrer Website

Damit der Einsatz der etracker Technologie auf Ihrer Website für Ihre Besucher transparent ist und diese über den Einsatz von etracker informiert sind, haben wir in Zusammenarbeit mit einer auf IT-Recht und Datenschutz spezialisierte Anwaltskanzlei eine Vorlage für Sie erarbeitet, die die Anforderungen von Art. 13,14 EU-DSGVO erfüllt.

Für die Ausübung der geforderten Widerspruchsmöglichkeit stellen wir Ihnen in Ihrem Account einen Button zum einfachen Einbau in Ihre Website zu Verfügung. Daneben können Sie auch die von uns bereitgestellte Schnittstelle nutzen, um den Widerspruch in eigene Dialoge zu integrieren.

Sollte die Datenverarbeitung vom Einwilligungserfordernis umfasst sein, weil Sie beispielsweise hochsensible oder personenbezogene Daten per Parameter an etracker übergeben oder die Daten für „unübliche“ Zwecke weiterverarbeiten, so können Sie das optionale Tracking-Opt-In in Ihren Einstellungen aktivieren oder die dazugehörige Schnittstelle verwenden.

✓ Technischer und organisatorischer Datenschutz bei etracker

Der Betrieb komplexer technologischer Infrastrukturen ist unsere Kernkompetenz und elementarer Bestandteil unserer Dienstleistung. Daher ist es unser oberstes Gebot, dass unser Rechenzentrum immer nach den aktuellsten Sicherheitsstandards betrieben wird. Dazu zählen neueste Firewall- und Intrusion-Detection-Technologien genauso wie umfangreiche physische Kontrollen und Zugangsbeschränkungen. Auf Applikationsebene finden moderne Authentifizierungsmethoden für Nutzer- und Administrator-Berechtigungen ebenso statt wie tägliche Backups sämtlicher Daten und deren dezentrale Archivierung.

Darüber hinaus werden alle in den etracker Produkten erfassten Daten in regelmäßigen Abständen vom Unternehmen Trustwave durch sogenannte „Penetrationstests“ auf ihre Sicherheit hin geprüft. Bei der Erfassung der Daten und dem Zugriff auf unsere Applikation wird zudem stets die „Secure Socket Layer“ (SSL)-Übertragung angewendet. Alle mit dieser Methode übertragenen Informationen werden verschlüsselt, bevor sie gesendet werden.

Genauso selbstverständlich wie die Verwendung neuester Sicherheitstechnologien ist für uns die Verpflichtung unserer Mitarbeiter/innen zur Verschwiegenheit und auf das Datengeheimnis. Die Verpflichtungen besteht auch nach Beendigung des Arbeitsverhältnisses fort. Zudem finden regelmäßige Schulungen zum Datenschutz statt.

Zeigen auch Sie Ihren Website-Besuchern und Kunden, dass Ihnen Datenschutz wichtig ist

Damit Sie Ihren Website-Nutzern und Kunden zeigen können, dass Sie verantwortungsvoll mit deren Daten umgehen, können Sie das etracker Privacy-Signet in Ihre Website, beispielsweise in den Datenschutzhinweisen, integrieren.

Wir stehen Ihnen gern Rede und Antwort zu Ihren Fragen zum Datenschutz. Wenden Sie sich hierzu jederzeit an unsere **Datenschutzbeauftragte Elke Hollensteiner** unter +49 40 55 56 59 52 oder **privacy@etracker.com**.