DSGVO:
Keine Revolution, sondern Evolution

Rechtlicher Hinweis
Dieser Artikel bietet lediglich allgemeine Informationen zum Thema und stellt keinen Ersatz für eine individuelle rechtliche Beratung dar. Für diese wenden Sie sich bitte an einen darauf spezialisierten Anwalt oder Ihre interne Rechtsabteilung.

Einleitung

Die EU-Datenschutz-Grundverordnung (DSGVO) harmonisiert die Datenschutzgesetzgebung in allen 28 Mitgliedstaaten der EU und ersetzt damit die Datenschutzrichtlinie von 1995.

Seit Gründung des Unternehmens im Jahr 2005 war es stets zentrale Firmenpolitik, unsere Technologie auf die höchsten Anforderungen von Datenschutz und -sicherheit abzustimmen und gleichzeitig unsere Kunden darin zu unterstützen, ihren Käufern personalisierte, relevante Werbung zu bieten. Criteo ist ein international tätiges Unternehmen mit Niederlassungen in zahlreichen Ländern der EU; wir arbeiten mit Tausenden von Werbetreibenden und Publishern zusammen, deren Kunden und Nutzer gleichfalls in der EU ansässig sind. Es versteht sich daher von selbst, dass wir die rechtlichen Vorschriften und Auflagen in den jeweiligen Ländern zu erfüllen.

Unserer Meinung nach schaffen Konsistenz und Rechtssicherheit in den Bereichen Datenschutz und -sicherheit eine Win-Win-Situation für alle Beteiligten: für die Unternehmen und auch für die Konsumenten. Daher sieht sich Criteo bei der Compliance mit der DSGVO klar in der Pflicht; darüber hinaus arbeiten wir eng mit den Kunden und Partner zusammen, die ebenfalls von diesem neuen Regelwerk betroffen sind: Wir unterstützen sie bei der notwendigen Transformation und teilen unsere Best Practices mit ihnen. Criteo ist gut auf die Herausforderungen der DSGVO vorbereitet, daher erwarten wir – wenn überhaupt – nur minimale Auswirkungen auf die Zusammenarbeit mit unseren Kunden und Partnern.

Insgesamt betrachtet ist diese neue Regelung eine Evolution, die die Datenschutzvorschriften in den EU-Mitgliedschaften harmonisiert und gleichzeitig deren konsistente Anwendung und Durchsetzung durch die regionalen Datenschutzbehörden der einzelnen Länder möglich macht. Die Zielsetzungen der DSGVO sind klar definiert:

- Modernisierung des Rechtssystems zum Schutz persönlicher Daten im Zeitalter der Globalisierung und technologischen Innovation.
- Stärkung der Konsumentenrechte bei gleichzeitigem Abbau bürokratischer Hürden, um so einen freien Fluss von persönlichen Daten innerhalb der EU sicherzustellen.
- Klarheit und Konsistenz beim Thema Datenschutz sowie EU-weit konsistente Anwendung bzw. effektive Implementierung.

Wie definiert die DSGVO personenbezogene Daten?

Die DSGVO dient dem Schutz der Privatsphäre der EU-Bürger. Sie gilt für alle Unternehmen, die personenbezogene Daten von Bewohnern der EU sammeln und/oder verarbeiten – auch, wenn das Unternehmen selbst nicht in der Europäischen Union ansässig ist. Für die digitale Marketingbranche gilt es vor allem zu beachten, dass die die DSGVO für alle Informationen mit Personenbezug gilt; dazu gehören auch Online-IDs wie Cookies oder Advertising IDs. Diese Online-IDs werden in der Definition von personenbezogenen Daten ausdrücklich erwähnt; auch das zeigt, dass die neue EU-Gesetzgebung die Definition von personenbezogenen Daten besonders weit fasst.

An dieser Stelle ist es wichtig, darauf hinzuweisen, dass viele nationale Datenschutzbehörden in der EU solche Online-IDs bereits zu den personenbezogenen Daten zählen. Es handelt sich dabei also um keine neue Anforderung für Criteo; wir sammeln zudem ausschließlich nicht sensible personenbezogene Daten in Form von Cookies. Daher sind wir mit solchen Unterscheidungen gut vertraut und haben bereits bewährte Prozesse zur Wahrung der Compliance etabliert, die uns gleichzeitig ermöglichen, unseren Kunden optimale Performance zu bieten.

Wenn es um Datenmanagement geht, stellen viele Unternehmen immer wieder die gleichen Fragen. Vor allem: Wie genau definiert die DSGVO personenbezogene Daten? Personenbezogen sind alle Daten, die Folgendes enthalten:

- Informationen, die eine direkte Identifizierung möglich machen – zum Beispiel Namen, Vornamen, Telefonnummern usw.
- Pseudonymisierte Daten oder Informationen, die keine direkte Identifizierung von Nutzern erlauben, die es aber möglich machen, das Verhalten von einzelnen Nutzern zu erfassen (um ihr oder ihm zum Beispiel im richtigen Moment die richtige Werbung anzuzeigen)

Die EU-Datenschutz-Grundverordnung unterscheidet klar zwischen Informationen, die eine direkte Identifizierung ermöglichen, und pseudonymisierten Daten. Die EU-Datenschutz-Grundverordnung fördert die Nutzung pseudonymisierter Informationen; sie besagt ausdrücklich: „Der Einsatz von Pseudonymisierung bei der Verarbeitung von personenbezogenen Daten minimiert die Risiken für die Betroffenen und

unterstützt die Datenverantwortlichen dabei, ihre Verpflichtungen in Sachen Datenschutz zu erfüllen.“[1]

Sensible Daten sind alle Daten, die Informationen zu den folgenden Bereichen enthalten oder entsprechende Rückschlüsse erlauben:

- Ethnizität und Herkunft
- Politische Meinung
- Religion und Weltanschauung
- Mitgliedschaft in Gewerkschaften
- Genetische Daten
- Biometrische Daten, die dazu dienen, natürliche Personen eindeutig zu identifizieren
- Daten mit Bezug auf die Gesundheit, das Sexualleben oder die sexuelle Orientierung einer natürlichen Person

Daher sind die von Criteos Kunden und Partnern gesammelten und verarbeiteten Daten schon ihrer Natur nach nicht sensibel im Sinne der DSGVO. Criteo selbst sammelt ausschließlich pseudonymisierte technische IDs, die mit bestimmten Ereignissen im Onlineverhalten des jeweiligen Users verknüpft sind:

- Cookie IDs
- Gehashte E-Mail-Adressen
- Mobile Advertising IDs
- andere technische IDs, die Criteo erlauben, das Online-Verhalten von Personen individuell zu erfassen, ohne sie direkt identifizierbar zu machen

Was ist der Unterschied zwischen wirksamer und ausdrücklicher Einwilligung?

Die DSGVO etabliert zudem eine klare Unterscheidung zwischen wirksamer und ausdrücklicher Einwilligung der Betroffenen. Beide Formen der Einwilligung erfordern zwar eine aktive Willensbekundung der Betroffenen; „ausdrückliche Einwilligung“ impliziert jedoch eine sehr enge Auslegung dessen, was eine solche Willensbekundung darstellt: zum Beispiel die Auswahl einer Checkbox oder das Klicken auf einen „Zustimmen“-Button. Eine solche ausdrückliche Einwilligung ist ausschließlich beim Erfassen und Verarbeiten von sensiblen personenbezogenen Daten notwendig – wie zum Beispiel Ethnizität, Religion, sexueller Orientierung, politischer Meinung oder Gesundheitszustand.

Im Gegensatz dazu werden Online-IDs (wie zum Beispiel Cookies) ausdrücklich als nicht sensible personenbezogene Daten kategorisiert, erfordern also sicher eine wirksame, aber keine explizite Einwilligung.

[1] *DSGVO – Abschnitt 28*

Was bedeutet das und welche Konsequenzen hat es für euer Unternehmen?

Die EU-Datenschutz-Grundverordnung definiert sechs Rechtsgrundsätze für das Sammeln und Verarbeiten von personenbezogenen Daten in Europa. Wenn euer Unternehmen also solche Daten sammelt und/oder verarbeitet, unabhängig von der Art, muss dies auf einer Rechtsgrundlage geschehen, die die folgenden Faktoren einbezieht:

1. Lebenswichtige Interesse des Einzelnen
2. Öffentliches Interesse
3. Erfüllung eines Vertrages
4. Erfüllung von rechtlichen Verpflichtungen
5. Wirksame Einwilligung des Einzelnen
6. Berechtigtes Interesse des Datenverantwortlichen

Alle sechs Grundsätze haben den gleichen rechtlichen Wert, d. h. sie sind unabhängig voneinander. Für Unternehmen, die im Marketing oder digitalen Marketing tätig sind und/oder zu diesem Zweck Daten sammeln, sind vor allem zwei dieser Rechtsgrundsätze entscheidend:

1. Wirksame Einwilligung des Einzelnen
2. Berechtigtes Interesse des Datenverantwortlichen

Der aus unserer Sicht wichtigste Rechtsgrundsatz für unsere Kunden und Partner, die personenbezogene Daten (einschließlich technischer IDs) sammeln, ist die sogenannte „wirksame Einwilligung“.

Das Einholen von wirksamen Einwilligungen im Rahmen von Cookie-Retargeting ist in Europa bereits seit 2009 die Regel – seit der Einführung der ePrivacy Direktive (auch Cookie-Direktive genannt). Die Kunden und Publisher-Partner von Criteo, die keine sensiblen Daten verarbeiten, sondern ausschließlich mit über technische IDs erfasste Informationen zum Surf- und Kaufverhalten sowie zur Shopping-Historie arbeiten, erfüllen diese Anforderungen also bereits.

Wir erwarten, dass die Regeln zu einer wirksamen Einwilligung eine weitere Evolutionsstufe der bereits recht strengen Regeln in Europa darstellen werden. Die französische Datenschutzbehörde CNIL (die auch für die Überwachung von Criteo zuständig ist) hat die gleichen Empfehlungen zum Einholen der wirksamen Einwilligung von Konsumenten[2] ausgesprochen; sie empfiehlt mehrere, für die zuständigen Website-Administratoren einfach zu implementierende technische Lösungen.

---

[2] *CNIL: “Cookies : comment mettre mon site web en conformité?” https://www.cnil.fr/fr/cookies-comment-mettre-mon-site-web-en-conformite (nicht auf Deutsch/englisch verfügbar)*

Die von der EU-Datenschutz-Grundverordnung definierten Regeln für eine gültige eindeutige Einwilligung entsprechen im Großen und Ganzen den Vorgaben aus einer früheren Arbeitsunterlage der Artikel-29-Datenschutzgruppe[3]:

> ***Spezifische Informationen:*** *Die Einwilligung ist nur dann gültig, wenn sie für den konkreten Fall gegeben wurde und auf angemessener Information beruht. Das heißt mit anderen Worten, dass eine pauschale Einwilligung ohne Angabe des genauen Zwecks der Verarbeitung nicht zulässig ist.*
>
> ***Zeitablauf:*** *Grundsätzlich ist die Einwilligung vor Beginn der Verarbeitung einzuholen.*
>
> ***Aktive Entscheidung:*** *Die Einwilligung muss eindeutig sein. Folglich darf das Verfahren zur Einholung und zur Erteilung der Einwilligung keinen Zweifel an der Absicht der betroffenen Person lassen. Grundsätzlich bestehen keine Einschränkungen hinsichtlich der Form einer Einwilligung. Damit die Einwilligung gültig ist, muss sie jedoch durch eine aktive Willensbekundung des Nutzers erteilt werden. Als Mindestform der Willensbekundung könnte jede Art von Zeichen angesehen werden, das ausreichend eindeutig ist, um die Wünsche der betroffenen Person zum Ausdruck zu bringen und für den für die Datenverarbeitung Verantwortlichen verständlich zu sein (beispielsweise eine handschriftliche Unterschrift unter einem Papiervordruck oder ein aktives Verhalten, aus dem nach vernünftigem Ermessen auf eine Einwilligung geschlossen werden kann).*
>
> ***Ohne Zwang:*** *Eine Einwilligung kann nur dann gültig sein, wenn die betroffene Person eine echte Wahlmöglichkeit hat und keine Gefahr einer Täuschung, Einschüchterung, Nötigung oder beträchtlicher negativer Folgen besteht, wenn sie die Einwilligung nicht erteilt.*

Inwiefern lässt sich der Grundsatz „berechtigtes Interesse des Datenverantwortlichen“ anwenden?

Für ein berechtigtes Interesse muss der Zweck der Datenverarbeitung von den Usern nach vernünftigem Ermessen erwartbar sein. Die Verarbeitung von personenbezogenen Daten für Zwecke des Direktmarketings lässt sich daher als berechtigtes Interesse betrachten. Dieses berechtigte Interesse wiegt jedoch nicht schwerer als die grundlegenden Rechte der Konsumenten in den Bereichen Datenschutz und Wahrung der Privatsphäre. Es ist also notwendig, angemessene Sicherheitsmaßnahmen zu implementieren, mit denen potentielle Risiken für die Privatsphäre der User adressiert werden.

Bevor sich ein berechtigtes Interesse geltend machen lässt, müssen daher die folgenden grundlegenden Standards erfüllt sein:

- Es müssen Informationen bereitgestellt werden, die erläutern, welche Daten gesammelt werden, zu welchem spezifischen Zweck, und welche

---

[3] Artikel-29-Datenschutzgruppe: Arbeitsunterlage 02/2013 mit Leitlinien für die Einholung der Einwilligung zur Verwendung von Cookies: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp208_de.pdf

Auswirkungen diese Datensammlung auf die Online-Erfahrung des Users hat. Zum Beispiel:

„Unsere Website/App verwendet Cookies bzw. Advertising IDs für den Zweck der Werbung. So sind wir in der Lage, unsere Werbung den Usern von Partner-Websites und Apps zu zeigen, die Interesse an unseren Produkten haben. Retargeting-Technologie verwendet Cookies oder Advertising IDs, um Werbung anzuzeigen, die auf Ihrem Surfverhalten basieren. Weitere Informationen finden Sie in unseren Datenschutzrichtlinien. Dort erfahren Sie auch, wie Sie zielgerichtete Werbung durch uns deaktivieren können.“§ [Link zur Datenschutzrichtlinie des Partners] § Criteo Datenschutzrichtlinie: http://www.criteo.com/de/privacy/]

- Den Usern muss eine Kontrollmöglichkeit an die Hand gegeben werden, mit der sie ihre Erfahrung steuern können; diese muss auch ein Opt-Out beinhalten. Diese Kontrollmöglichkeit muss einfach zu nutzen und leicht zugänglich sein sowie über Erläuterungen verfügen, wie sich potentielle Einstellungsänderungen auf die Werbeerfahrung des Users auswirken.
- Die Datenschutzrichtlinien des Unternehmens müssen einfach zugänglich sein; ebenso Informationen zu Branchenstandards in diesem Bereich oder zu entsprechenden Selbstverpflichtungen Ihres Unternehmens. Beispiel: Criteo ist Mitglied der Network Advertising Initiative.

Um berechtigtes Interesse zu etablieren, sollten Unternehmen in der Lage sein, die folgenden Schlüsselfragen zu beantworten:

- Was ist der Zweck der Datensammlung und -verarbeitung?
- Ist sie notwendig, um eines oder mehrere spezifische Unternehmensziele zu erreichen?
- Erkennt die EU-Datenschutz-Grundverordnung oder die nationale Gesetzgebung im jeweiligen Land diese Art der Datenverarbeitung in Abhängigkeit des positiven Ergebnisses einer Abwägungsprüfung als berechtigt an?
- Muss der Betroffene unter normalen Umständen mit solch einer Erfassung und Verarbeitung seiner Daten rechnen?
- Welche Art von Daten werden verarbeitet? Unterliegt diese Art von Daten irgendwelchen spezifischen Schutzregelungen der EU-Datenschutz-Grundverordnung?
- Beschneidet oder unterminiert das Erfassen und Verarbeiten der Daten die Rechte der Betroffenen?
- Wird der Betroffene angemessen auf die Erfassung und Verarbeitung seiner Daten hingewiesen? Wenn ja, wie? Sind diese Hinweise ausreichend klar formuliert und beschreiben auch angemessen den Zweck der Verarbeitung?

Privacy by Design – Criteos Ansatz zum Datenschutz

Datenschutz und die Wahrung der Privatsphäre sind wesentliche Leitprinzipien unserer Arbeit bei Criteo. Wir betreiben großen Aufwand, um die von uns erfassten Daten zu schützen und ausschließlich in Übereinstimmung mit den jeweils gültigen Datenschutzgesetzen zu verarbeiten. Das schließt selbstverständlich auch die Bestimmungen der DSGVO ein.

Bei der Entwicklung von neuen Produkten und Features sind Datenschutz und Wahrung der Privatsphäre stets zentrale Prinzipien; das ist ein wesentlicher Grundpfeiler von Privacy by Design: Mit diesem hochmodernen Ansatz bieten wir ein marktführendes Sicherheitsniveau – und zwar für Werbetreibende und Konsumenten gleichermaßen.

Unter der Bezeichnung **Privacy by Design** haben wir die zahlreichen Richtlinien und Maßnahmen von Criteo zusammengefasst, mit denen wir branchenführenden Datenschutz sowie Sicherheit sowohl für Konsumenten als auch für Werbetreibende sicherstellen. Zu den wesentlichen Elementen gehören:

- Wie in der EU-Datenschutz-Grundverordnung vorgeschrieben, haben wir einen hauptamtlichen Datenschutzbeauftragten ernannt. Er arbeitet mit einem Team von Datenschutzexperten.
- Diese Experten sind Mitarbeiter der Produkt-Abteilung sowie der Forschung und Entwicklung. Mit kontinuierlichen Assessments im Bereich Datenschutz beobachten sie potentielle Risiken über den gesamten Produkt-Lebenszyklus hinweg und adressieren diese Risiken proaktiv.
- Das Datenschutzteam bietet unternehmensweite Trainings in diesem Bereich, setzt entsprechende Verhaltensregeln durch und ist so entscheidend an der überragenden Qualität unserer Produkte beteiligt.
- Wir überprüfen und dokumentieren unsere internen Richtlinien regelmäßig und aktualisieren alle Datenschutzrichtlinien, falls nötig. Unsere Partner und Lieferanten sind gleichfalls vertraglich verpflichtet, diese Richtlinien einzuhalten.

Strikte Sicherheitsmaßnahmen

In Übereinstimmung mit der DSGVO setzt Criteo beim Sammeln der Konsumentendaten in Zusammenarbeit mit unseren Kunden auf strikte Sicherheitsmaßnahmen. Wir verwenden modernste Pseudonymisierungs-Methoden wie zum Beispiel Hashing-Prozesse, die im Rahmen der DSGVO als Best Practices anerkannt sind. Zudem speichern wir niemals wissentlich personenbezogene Daten, mit denen sich einzelne Konsumenten exakt identifizieren lassen. Aus Gründen der Compliance und Performance speichern wir die Daten von Konsumenten aus der EU im physisch nächstgelegenen Rechenzentrum innerhalb der Grenzen der EU.

Ad Choices: Ein Programm mit Schwerpunkt auf den Rechten und Kontrollmöglichkeiten der Konsumenten

Criteo hat schon vor langer Zeit erkannt: Es ist notwendig, eine Balance zwischen relevanter Werbeerfahrung und Wahrung der Privatsphäre zu schaffen; zudem gilt es, Konsumenten entsprechende Kontrollmöglichkeiten an die Hand zu geben.

Die Konsumenten verstehen diese Art des Austauschs. Daher ist Criteo bereits seit 2008 engagiert im Programm „Ad Choices“: Es erlaubt Konsumenten mit einem einzigen Mausklick zu sehen, wo Criteo Daten nutzt und wie wir die Privatsphäre der User schützen. Entscheidet sich ein Konsument für ein Opt-Out, stellen wir das Tracking und Retargeting unmittelbar ein. Anschließend entfernen wir alle IDs aus den Browsern der Betroffenen, sodass wir sie auch in Zukunft nicht mehr tracken können. Den Schutzregelungen der EU entsprechend werden alle personenbezogenen Daten von Konsumenten für maximal 13 Monate gespeichert.

Führend in unserer Branche: Investitionen in Standards und Zertifizierungen

Criteo verfügt bereits über eine große Zahl von Zertifizierungen, die jährlich von Behörden und anderen Kontrollinstanzen überprüft werden. Unter anderem:

- Network Advertising Initiative Standards
- IAB Europe
- Digital Advertising Alliance: Selbstregulierungskodex für verhaltensbasierte Online-Werbung
- European Digital Advertising Alliance: Selbstregulierungskodex
- Digital Advertising Alliance of Canada: Selbstregulierungskodex
- TrustArc Trusted Data Collection Zertifizierung

Ist Euer Unternehmen bereit für die DSGVO?

Die DSGVO gilt für alle Unternehmen, die entweder in der EU ansässig sind oder Daten aus dem EU-Raum verarbeiten. Die zahlreichen, teilweise neuen Regularien gelten also auch für internationale Unternehmen mit Hauptsitz außerhalb der EU, die Kunden im EU-Raum ansprechen wollen. Unserer Meinung nach werden übrigens die meisten Unternehmen letztendlich von der DSGVO profitieren: Die neue Gesetzgebung harmonisiert die rechtliche Situation in allen 28 Mitgliedsstaaten der EU. Criteo unterstützt seine Kunden und Partner bei der Einhaltung der Compliance mit der DSGVO: Wir stellen Informationen und Best Practices sowie individuelle Beratung zur Verfügung.

Die folgenden Best Practices solltet Ihr unbedingt umsetzen:

Ernennung eines Datenschutzbeauftragten

In den folgenden Fällen verlangt die EU-Datenschutz-Grundverordnung zwingend die Ernennung eines Datenschutzbeauftragten:

- Die Datenverarbeitung erfolgt durch eine **Behörde oder öffentliche Institution** – mit Ausnahme von Gerichten in Ausübung ihrer Tätigkeit.
- Die zentralen Aufgaben des Controllers oder der Datenverarbeitung umfassen Prozesse, **die ihrer Natur, ihrem Umfang oder ihrem Zweck nach die regelmäßige und systematische Überwachung von Datensubjekten in großen Maßstab beinhalten**.
- Oder: Die zentralen Aufgaben von Controlling und Datenverarbeitung umfassen die **Verarbeitung von sensiblen Daten in großem Maßstab** (zum Beispiel Daten zu Ethnizität, Herkunft, Religion, Weltanschauung, Gesundheit, sexuellen Präferenzen usw.) oder von persönlichen Daten mit Bezug auf Straftaten bzw. strafrechtlichen Verurteilungen.

Der Datenschutzbeauftragte ist für Überwachung und Management sowohl der Daten als auch der Prozesse zuständig und muss dafür sorgen, dass alle Regeln und Vorschriften eingehalten werden. Für den Datenschutzbeauftragten darf zudem nachweislich kein Interessenskonflikt in Hinblick auf den Datenschutz in eurem Unternehmen bestehen.

Der Datenschutzbeauftragte muss auf seine Tätigkeit und vor allem auf die notwendige Zusammenarbeit richtig vorbereitet sein

Sollte es aktuell Mängel und Probleme im Datenschutz eures Unternehmens geben, sind eure Mitarbeiter die beste Informationsquelle. Ihr müsst also sicherstellen, dass der Datenschutzbeauftragte ebenso wie die für Rechtsfragen, Compliance und IT zuständigen Mitarbeiter genaue und umfassende Kenntnis der Datenverarbeitung in eurem Unternehmen haben. Hand in Hand sollten sie einen rechtlich verlässlichen Prozess zur kollaborativen Datenerfassung schaffen.

Transparenz und Kontrolle

Alle Informationen, die ihr euren Kunden zur Verfügung stellt, sollten so klar und transparent wie möglich formuliert sein. Das gilt selbstverständlich auch für die notwendigen Zustimmungserklärungen. Eure Website sollte euren Kunden explizit erklären, welchen Datenerhebungen sie in welchem Umfang zustimmen, bzw. ablehnen, was die jeweiligen Konsequenzen sind und welche Daten sie euch zur Verfügung stellen. Das ist ein zentraler Aspekt der EU-Datenschutz-Grundverordnung.

Daten-Governance muss an erster Stelle stehen

Für alle Schritte der Datenverarbeitung, die möglicherweise negativ in die Persönlichkeitsrechte von Betroffenen eingreifen, solltet ihr einen Prozess zur Überprüfung des Datenschutzes etablieren. Zudem sollte euer Unternehmen nicht nur in allen Fällen erklären können, wie persönliche Daten gesammelt, genutzt und möglicherweise sogar verändert werden, sondern auch Prozesse bereitstellen, mit deren Hilfe EU-Bürger Daten einfach einsehen, korrigieren oder löschen lassen können. Die DSGVO schreibt zwingend vor, dass die Daten-Infrastruktur eures Unternehmens Datenverarbeitungsprozesse protokolliert. Zudem sollten eure Unternehmensprozesse möglichst vollständig transparent sein.

Kontrolle des Datenzugriffs durch Mitarbeiter und Arbeitspartner

Mitarbeiter und Partner dürfen nur in dem Umfang Zugriff auf eure Daten haben, in dem dies im Rahmen ihrer Tätigkeit notwendig ist. Deswegen müsst ihr strikte Autorisierungsprozesse etablieren. Eure Datenschutzrichtlinien sollten auf Basis des Bedarfs eures Unternehmens kontinuierlich aktualisiert und engmaschig auf ihre Einhaltung hin kontrolliert werden – insbesondere bei Datentransfers.

Kapitel V der EU-Datenschutz-Grundverordnung schreibt zudem vor, dass Empfänger von Daten, die außerhalb des EU-Raumes ansässig sind, die gleichen Datenschutz- und Governance-Vorschriften erfüllen müssen wie Unternehmen innerhalb der EU. Die Anforderungen der DSGVO sind streng; richtig darauf vorbereitet zu sein, verlangt jedoch mehr als nur das abhaken einer Checkliste gemeinsam mit den Anbietern, mit denen er zusammenarbeitet. Unserer Meinung nach bietet die DSGVO jedoch sowohl Unternehmen wie auch Konsumenten klare Vorteile: Sie schafft Konsistenz und Rechtssicherheit bei den Themen Datenschutz und Privatsphäre.

Wie wirkt sich die DSGVO auf das Lösungsportfolio von Criteo aus?

Ein wesentlicher Kern unserer Technologie ist der Criteo Shopper Graph, der Daten zum Kaufverhalten aus unserem Netzwerk sammelt. Der Shopper Graph ist wesentlicher Bestandteil all unserer Produkte im Criteo Commerce Marketing Ecosystem. Er untergliedert sich in drei vertrauenswürdige Datenkollektive, in denen drei Arten von Käuferdaten kombiniert werden:

- „Pseudonymisierte“ technische IDs
- Interessen hinsichtlich der Produkte und Services unserer Kunden
- Messwerte und Statistiken zur Performance unserer Services

Wir sorgen kontinuierlich dafür, dass die so erfassten Daten strikt auf das begrenzt sind, was unsere Services wirklich benötigen, um Käufern relevante Informationen zu den Produkten zu zeigen, die für sie interessant sind – am richtigen Ort und mit der richtigen Botschaft. Zum Beispiel:

- Wir setzen ausschließlich modernste Hashing-Mechanismen ein, um eine besonders starke Pseudonymisierung zu gewährleisten.
- Wir speichern Daten grundsätzlich nur für begrenzte Zeit und niemals länger, als unbedingt nötig. Dabei beachten wir die Empfehlungen der EU-Datenschutzbehörden zu Cookies und digitaler Werbung.
- Wir stellen nutzerfreundliche Wahlmechanismen zur Verfügung. Für alle Criteo-Produkte besteht der gleiche einfache Opt-Out-Prozess, der über all unsere Ads und über unsere Datenschutzrichtlinien erreichbar ist. Darüber hinaus sind wir registrierte Mitglieder der Opt-Out-Plattformen von NAI, DAA und IAB Europa, über die User dem gezielten Targeting durch uns widersprechen können:
- Über den Ad Choices Link in unseren Ads haben Konsumenten eine ganz einfache Möglichkeit zum Opt-Out aus unseren Services. Sobald ein User sich für diese Möglichkeit entscheidet, werden alle gespeicherten Informationen gelöscht oder

unzugänglich gemacht – einschließlich aller Nutzerdaten, die unsere Kunden im Rahmen einer Kampagne mit Criteo-Produkten möglicherweise hochgeladen haben.

EU-Bürger erwarten relevante Werbung – ein Schlusswort

Unternehmen aus der Digital Marketing-Branche, die aktuell ihre Firmenpolitik auf die DSGVO abstimmen, sollten sich jedoch bewusst sein, dass die EU-Bürger sehr genau wissen, dass es zielgerichtete Werbung gibt; sie verstehen die Funktionsweise der IDs dahinter (zum Beispiel Cookies) und sie erwarten, für sie relevante Werbung sehen. In Zusammenarbeit mit IPSOS[4] hat Criteo eine Konsumentenbefragung durchgeführt, um die Erwartungshaltungen von Usern aus der EU mit Hinblick auf zielgerichtete Online-Werbung besser zu verstehen. Für diese Studie wurde in Frankreich, Großbritannien und Spanien eine mit Bezug auf Geschlecht, Alter, Region und Einkommen repräsentative Gruppe von 3000 Internetnutzern im Alter zwischen 16 und 65 befragt:

- 90 % der Internetnutzer sind sich bewusst, dass es verhaltensabhängiges Retargeting gibt.
- 68 % der Internetnutzer wissen, dass Cookies zielgerichtete Werbung ermöglichen.
- 75 % erwarten, dass die ihnen gezeigten Anzeigen ihren Interessen entsprechen.
- 73 % ziehen es vor, relevante Anzeigen zu sehen, statt für die Werbefreiheit eines Angebots zu bezahlen.

Bei Criteo sind wir der festen Überzeugung, dass der Datenschutz für Konsumenten sowie Klarheit und Transparenz bei den Geschäftspraktiken für alle Seiten klare Vorteile bietet. Wenn Kunden genau verstehen, wofür die von ihnen gesammelten Informationen verwendet werden und zudem die Kontrolle über die Daten zu ihrem persönlichen Surf-Verhalten behalten, gewinnen sie Vertrauen zu den Unternehmen – und das steigert letztendlich die Kundenbindung.

Wir kennen die Implikationen der DSGVO genau und sind darauf vorbereitet; gerne helfen wir unseren Kunden und Partnern dabei, unsere Produkte und Dienstleistungen besser zu verstehen. je intensiver wir gemeinsam daran arbeiten, die neue Gesetzgebung zu verstehen und umzusetzen, desto früher kehrt wieder der Alltag in unser Geschäft ein.

[4] *Criteo-IPSOS Studie, 2017*