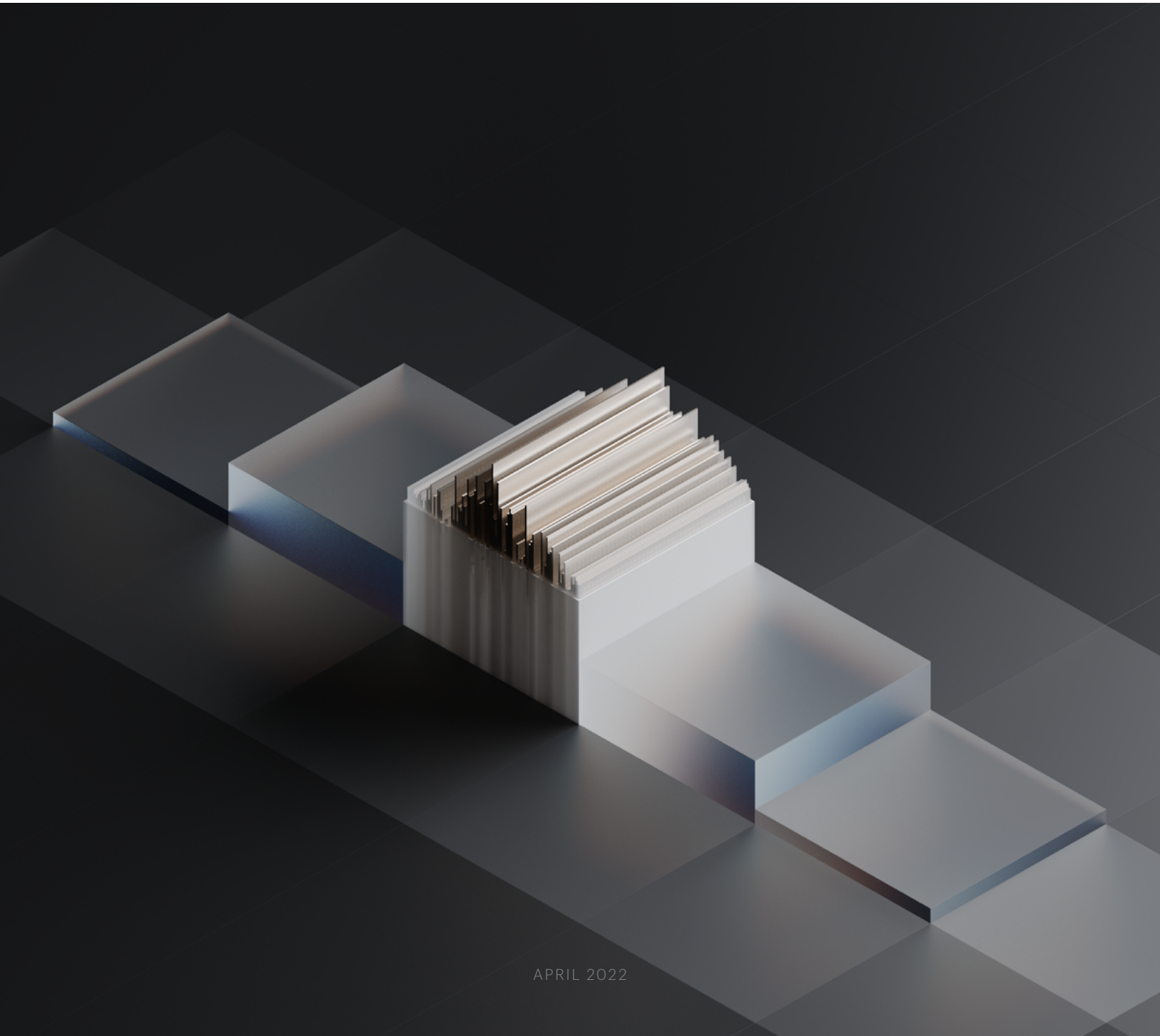
piano analytics

Datenschutz steht an erster Stelle

Aufbau einer Datenanalysestrategie, die mit den EU-Datenschutzgesetzen konform ist



APRIL 2022

Aufgliederung des Datenschutzes

Das erste wirkliche Zeichen für den bevorstehenden Wandel kam im Dezember 2021.

Zu der Zeit entschied die österreichische Datenschutzbehörde gegen das Gesundheitsportal NetDoktor. Die Behörde stellte fest, dass die Verwendung von Google Analytics gegen die Datenschutzgrundverordnung der Europäischen Union (DSGVO) verstößt.

Allerdings hatte NetDoktor Google Analytics nicht auf ungewöhnlichen Weise verwendet. Durch die Verwendung von Cookies konnten sie den Besuch der Nutzer ihrer Website verfolgen und dadurch besser verstehen, welche Seiten ihre Nutzer besucht haben, wie viel Zeit sie auf der Website verbracht haben und vieles mehr. Diese Daten wurden über eine Identifikationsnummer mit anderen Daten desselben Nutzers verknüpft, um ein umfassenderes Bild von jedem einzelnen Besucher zu erhalten. Unternehmen aus der ganzen Welt verwenden das Instrument auf genau dieselbe Art und Weise.

Wie als Beweis dienend hat die französische Datenschutzbehörde Commission Nationale de l'Informatique et des Libertés (CNIL) im Februar 2022 eine ähnliche Entscheidung gegen ein anderes Unternehmen getroffen. Liechtenstein hat im März 2022 eine eigene Regelung angekündigt.

NetDoktor war nicht das Problem, das war klar. Jedenfalls nicht ausschließlich.

Die Datenschutzbehörden waren sich einig, dass Google Analytics – und damit auch jedes Unternehmen, das es verwendet – gegen die Datenschutzbestimmungen der Europäischen Union verstößt, indem es die Übermittlung europäischer Nutzerdaten in die Vereinigten Staaten ohne entsprechende Garantien zulässt. Die Vorschriften gegen diese Art der Datenübermittlung besagen, dass europäische Nutzerdaten dadurch Angriffen von US-Strafverfolgungs- und Spionagebehörden ausgesetzt werden könnten. Aber was bedeutet das überhaupt? Und was sind die Auswirkungen auf Unternehmen, die digitale Analysen einsetzen?

Die weitreichenden Auswirkungen

Für diejenigen, die sich mit Datenschutzgesetzen beschäftigen, kamen die Entscheidungen in Europa nicht völlig überraschend.

Nur anderthalb Jahre zuvor, im Juli 2020, war das „Privacy Shield“, das von vielen zum Schutz von Daten beim Datenaustausch zwischen der Europäischen Union (EU) und den USA genutzt wurde, vom Gerichtshof der Europäischen Union für rechtswidrig erklärt worden. Als die Urteile ergangen sind, hatte man sich noch nicht auf einen vernünftigen Ersatz geeinigt. Nach Ansicht europäischer Beamter waren die Daten dadurch unsicher.

Jetzt besteht für jedes Unternehmen, das Google Analytics verwendet, die Gefahr der Nichteinhaltung von Vorschriften. Und das nicht nur in Frankreich, Österreich und Liechtenstein. Es wird angenommen, dass dies eine Reihe von Entscheidungen nach sich ziehen wird.

„Wir erwarten im Laufe der Zeit ähnliche Entscheidungen in den meisten EU-Mitgliedsstaaten", erklärte Max Schrems im Januar 2022. Schrems ist der Ehrenvorsitzende von noyb (None of Your Business – übersetzt in etwa: „das geht dich nichts an"), der Datenschutzvereinigung, die das Problem der Datenübermittlung ursprünglich an die europäischen Behörden herangetragen hat. „Wir haben 101 Beschwerden in fast allen Mitgliedstaaten eingereicht, und die Behörden haben die Reaktion koordiniert."

Diese Urteile betreffen Google-Analytics-Nutzer nicht nur in Europa, sondern weltweit, so dass jedes Tool oder Unternehmen, das Daten in ähnlicher Weise verwendet, dem Risiko einer möglichen Nichteinhaltung ausgesetzt ist.

„Die DSGVO gilt für europäische Unternehmen sowie für Unternehmen, die mit europäischen Daten arbeiten", erklärt Louis-Marie Guérif, Datenschutzbeauftragter der Piano Gruppe und Datenspezialist in Frankreich. „Also muss mehr oder weniger jeder, der in Europa und mit europäischen Daten zu tun hat, die DSGVO respektieren."

Das bedeutet, dass Unternehmen diesbezüglich weltweit vor der Wahl stehen.

Die Bedeutung der EU-Datenschutzvorschriften für Unternehmen

Für jedes Unternehmen, das bei seiner Entscheidungsfindung auf Nutzerdaten angewiesen ist – also für die meisten Unternehmen heutzutage – haben die Nachrichten aus Europa potenziell nachhaltige Auswirkungen. Selbst diejenigen, die nur wissen wollen, wie viele Besucher auf ihre Website kommen oder welche Seiten am beliebtesten sind, sind davon betroffen. „Dies ist ein Thema, das alle Aspekte der Wirtschaft und des gesellschaftlichen Lebens betrifft", erklärte Gabriela Zanfir-Fortuna, Vizepräsidentin für globalen Datenschutz bei der gemeinnützigen Denkfabrik Future of Privacy Forum, im Januar gegenüber Wired.

Wie Sie darauf reagieren, bleibt allerdings Ihnen überlassen. Sie könnten Google Analytics weiterhin verwenden, obwohl Sie wissen, dass es illegal ist, und hoffen, dass Google eines Tages die Vorschriften einhält (obwohl Google bisher keinerlei Anzeichen dafür gezeigt hat, dass es sich diesbezüglich bewegt). Man könnte hoffen, dass eine andere Version des Privacy Shields eingeführt wird – eine, die dieses Mal stark genug ist, um den EU-Vorschriften standzuhalten. Oder Sie finden eine andere digitale Analyselösung, die Ihnen die benötigte Funktionalität bietet und gleichzeitig mit dem europäischen Recht vereinbar ist.

„Ihre Antwort hängt von Ihrer Risikotoleranz ab", ergänzt Guérif. „Meine Empfehlung und die Empfehlung der Experten ist es, das Risiko zu bewerten, und wenn Sie sich der Meinung von CNIL und anderen Datenschutzbehörden anschließen, dann müssen Sie Alternativen bewerten und Wege finden, um das Risiko zu reduzieren."

Die Bewertung Ihres Risikos bedeutet aber auch, dass Sie die möglichen Auswirkungen der Nichteinhaltung von Vorschriften verstehen müssen – was mit der Möglichkeit hoher Geldstrafen und mehr verbunden ist. Es könnte sogar bedeuten, dass Sie den Zugriff auf die bereits gesetzwidrig gesammelten Besucherdaten verlieren.

Dieser Leitfaden richtet sich an diejenigen, die noch dabei sind, ihr Risiko zu bewerten und sich über die Folgen der Nichteinhaltung der Vorschriften informieren, sowie an diejenigen, die alternative Lösungen zur

Minimierung beider Probleme in Betracht ziehen. Es wird untersucht, was zu beachten ist, wenn Sie eine datenschutzfreundliche digitale Analysestrategie entwickeln, worauf Sie bei einer Lösung achten sollten, die die Einhaltung von Vorschriften priorisiert, und wie Sie Ihre Daten sicher migrieren können, wenn Sie sich für diesen Schritt entscheiden.

Aber lassen Sie uns zunächst einen Blick auf die Datenschutzgesetze werfen, die für Sie gelten.

Verständnis der EU-Datenschutzgesetze

Die jüngsten Urteile zeigen uns, dass die europäischen Datenschutzgesetze die Art und Weise, wie Sie Daten nutzen, beeinflussen können. Sie sind strenger als die US-Datenschutzgesetze und regeln, wie Sie personenbezogene Daten von europäischen Nutzern erfassen, weitergeben und speichern – unabhängig davon, ob Sie in Europa ansässig sind oder nicht. Wenn Sie also ein digitales Analysetool einsetzen oder den Einsatz planen, sollten Sie diese Gesetze verstehen.

Zwei verschiedene Datenschutzrichtlinien betreffen die Datenpraktiken in Europa. Schauen wir uns diese nacheinander an.

DSGVO

Die Datenschutz-Grundverordnung (DSGVO) ist Teil des Datenschutzrechts der Europäischen Union und regelt unter anderem die Übermittlung personenbezogener Daten außerhalb der EU und des Europäischen Wirtschaftsraums (EWR). Das bedeutet, dass Daten nicht in Länder ausgeführt werden dürfen, die nicht über ein „angemessenes Schutzniveau" verfügen, d.h. über das gleiche Niveau an Datenschutzvorschriften wie die EU.

Die im Mai 2018 in Kraft getretene Verordnung verlangt von Unternehmen, dass sie bei der Verwendung personenbezogener Daten transparent vorgehen, ihre Nutzer und Kunden über die von ihnen erhobenen Daten informieren, eine gesetzliche Grundlage zur Verarbeitung der Daten einholen und ihnen mitteilen, falls der Datenschutz verletzt wurde. DSGVO definiert personenbezogene Daten als:

„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann."

Auf Grundlage dieser Definition betrachten die wichtigsten Datenschutzbehörden daher Analyse- und

Besuchsdaten als personenbezogene Daten, die auch als solche behandelt werden müssen. Das bedeutet: Transparenz für die Nutzer darüber, was mit ihren Daten geschieht, das Recht, der Verarbeitung zu widersprechen, oder die Verpflichtung, diese Daten auf angemessene Weise zu schützen, mit möglichen Maßnahmen wie Pseudonymisierung und Anonymisierung.

ePrivacy

Dabei handelt es sich um eine europäische Richtlinie, die sich mit der elektronischen Kommunikation und unter anderem mit der Verwendung von so genannten Trackern befasst: Cookie-ID, Mobile-ID, Pixel, Fingerabdruck usw.

Gemäß ePrivacy dürfen Sie keine Informationen auf dem Endgerät eines Endnutzers lesen oder schreiben, d.h. einen Besucher oder Nutzer verfolgen, es sei denn, Sie erhalten entweder eine vorherige und ordnungsgemäße Zustimmung oder verfügen über eine spezifische Ausnahme.

Die Europäische Kommission hat einen neuen Entwurf für eine ePrivacy-Verordnung vorgelegt, der die ePrivacy Richtlinie aktualisieren soll, um eine vollständig harmonisierte Sichtweise der Datenverfolgung und der Vertraulichkeit in der elektronischen Kommunikation innerhalb der EU zu erhalten.

Weitreichende Auswirkungen

Die DSGVO und die ePrivacy-Verordnung mögen europäische Gesetze sein, aber – wie wir bereits gesehen haben – bedeutet das nicht, dass sie nur Unternehmen in der EU betreffen. Das Internet ist schließlich grenzenlos. „Als die DSGVO in Kraft trat, war eines der unmittelbaren Ergebnisse ein Anstieg der Zahl der US-Websites, die den Zugang zu EU-Besuchern verweigern oder einschränken“, erklärte Timo Rein, Mitbegründer und ehemaliger CEO des CRM-Anbieters Pipedrive, gegenüber Forbes kurz nach Inkrafttreten der DSGVO. „Dieser Ansatz ist nicht nachhaltig.“

Heute ist also praktisch jedes Unternehmen mit einer Website von der Datenschutz-Grundverordnung und dem Datenschutz auf elektronischem Wege betroffen – selbst wenn sie nur auf die grundlegendsten Daten der Zielgruppe zugreifen.

Das Risiko der Nichteinhaltung von Vorschriften

Die Verwendung von Daten in einer Weise, die gegen ePrivacy oder DSGVO verstößt, kann schwerwiegende Folgen haben. Wenn Sie die Vorschriften nicht einhalten, riskieren Sie eine Verwarnung, erhebliche Geldbußen von bis zu 20 Millionen Euro oder 4"% Ihres weltweiten Umsatzes und/oder ein vorübergehendes oder dauerhaftes Verbot der Verarbeitung personenbezogener Daten. Sie können auch gezwungen werden, alle von Ihnen bereits gesetzwidrig gesammelten Daten zu löschen.

Wenn Sie diese Risiken nicht eingehen wollen, ist es wichtig, eine durchdachte Datenstrategie zu entwickeln und einen Anbieter für digitale Analysen zu finden, der sich mit DSGVO und ePrivacy auskennt und über das nötige Fachwissen verfügt, um mit den gesetzlichen Anforderungen Schritt zu halten.

Schaffung einer Strategie für den Datenschutz

Die meisten Unternehmen wissen heute, wie wichtig digitale Analysen sind. Durch die Analyse des Nutzerverhaltens können Sie bessere geschäftliche Entscheidungen auf der Grundlage der Bedürfnisse Ihrer Zielgruppe treffen und bessere Nutzererlebnisse schaffen. Dazu benötigen Sie hochwertige Daten. Aber wenn Sie auch in Zukunft den Minen ausweichen, das Vertrauen der Nutzer aufrechterhalten und sich weiterhin erfolgreich durch die regulatorische Landschaft bewegen wollen, brauchen Sie eine langfristige Strategie für den Datenschutz – wie auch immer diese aussehen mag.

„Als Unternehmen sollten Sie sich mit Ihren Datenschutz- und Rechtsteams sowie mit allen Teams in Ihrem Unternehmen, die mit Daten zu tun haben, beraten", empfiehlt Guérif. „Treffen Sie nicht einfach eine schnelle Entscheidung, für die Sie möglicherweise erst in sechs oder zwölf Monaten bezahlen werden. Datenschutz ist ein Risikokonzept – man muss das Risiko abwägen, eine Geldstrafe zu bekommen, Daten zu verlieren oder seine Daten nicht nutzen zu können

Wenn Sie sich dafür entscheiden, der Einhaltung von Vorschriften langfristig Vorrang einzuräumen, müssen Sie wissen, worauf Sie bei der Suche nach einer geeigneten digitalen Analyselösung achten müssen.

Die versteckten Kosten kostenloser Tools (er)kennen

Trotz der wichtigen Rolle, die digitale Analysen spielen, geben viele Unternehmen bei der Auswahl einer Lösung immer noch Kosteneinsparungen gegenüber Funktionalität den Vorrang. Jedoch gibt es versteckte Kosten für kostenlose Tools, wie wir gerade in Europa beobachten können. Kosten, die den Datenschutz der Nutzer beeinträchtigen können.

Um diese Kosten zu verstehen, lassen Sie uns die beiden Arten von kostenlosen digitalen Analyselösungen, die derzeit verfügbar sind, aufschlüsseln.

Open Source und Vor-Ort

Open-Source-Lösungen für die digitale Analyse vor Ort sind die weniger verbreiteten der kostenlosen Alternativen. Und das aus gutem Grund – sie bieten nicht die gleichen komplexen Nutzerdaten, nach denen moderne Unternehmen suchen. Zusätzlich werden Sie für Ihre eigenen Sicherheits- und Datenschutz-Updates verantwortlich gemacht.

Das bedeutet, dass es Ihre Aufgabe ist, sich über DSGVO und ePrivacy auf dem Laufenden zu halten, ebenso wie über alle Änderungen in der Datenschutzlandschaft – sowie, Ihre Nutzung zu aktualisieren, wenn Sie die Vorschriften einhalten wollen. Wenn Sie nicht über die Ressourcen oder das Know-how verfügen, um auf dem Laufenden zu bleiben, riskieren Sie die Nichteinhaltung der Vorschriften.

Mit Daten den Preis zahlen

Die gängigsten kostenlosen Lösungen sind natürlich solche wie Google Analytics. Sie bieten moderne Besucherdaten, aber das ist mit einem Vorbehalt verbunden. „Das Problem bei kostenlosen Angeboten ist, dass Sie selbst das Produkt sind, also der Nutzer", erläutert Guérif.

Die von Ihnen gesammelten Kundendaten sind der Preis für den Eintritt und können auf eine Art und Weise verwendet werden, die sich Ihrer Kontrolle entzieht, wie z. B. für die Erstellung von Nutzerprofilen und digitale Werbung – und das alles ohne die Einwilligung der Nutzer. Außerdem kann es für Endnutzer schwierig sein, sich gegen die Datenverfolgung zu entscheiden und die Kontrolle über die Verwendung ihrer Daten zu übernehmen. Darüber hinaus verfügen Anbieter kostenloser Lösungen häufig nicht über spezielle Ressourcen und Unterstützung, um sicherzustellen, dass Sie die gesetzlichen Anforderungen wie die der DSGVO und ePrivacy erfüllen.

„Bei kleineren oder kostenlosen Lösungen ist es normal, dass keine Experten zur Verfügung stehen, mit denen man sprechen kann und die einem helfen, die Lösung rechtskonform zu konfigurieren", fügt Guérif hinzu. „Sie sind mehr oder weniger allein mit Ihrem kostenlosen Tool."

Suche nach einer datenschutzfreundlichen Analyselösung

Wenn die Kostenfreiheit für Sie jedoch nicht an erster Stelle steht, können Sie sich ein Tool suchen, das alle von Ihnen benötigten Funktionen und Datentypen enthält. Und Sie können sich dafür entscheiden, den Datenschutz an erster Stelle Ihrer Liste zu setzen.

Bei der Suche nach einer datenschutzfreundlichen digitalen Analyselösung sind zunächst die folgenden Punkte zu berücksichtigen.

Wie werden „personenbezogene Daten" definiert?

Erinnern Sie sich an die Definition von „personenbezogenen Daten" in der DSGVO? Wenn Sie eine Lösung wünschen, die die Vorschriften einhält, brauchen Sie einen Anbieter, der dieselbe Definition verwendet, d. h. der z. B. Cookie-/mobile IDs und IP-Adressen als personenbezogene Daten einbezieht. Wenn das Tool personenbezogene Daten nicht auf die gleiche Weise bezeichnet, besteht die Gefahr, dass es nicht den Vorschriften entspricht.

Verwendung und Speicherung von Daten

Bei den Entscheidungen in ganz Europa ging es vor allem darum, wo die Daten gespeichert werden und wie sie verwendet werden. Zur Einhaltung der DSGVO müssen die schützenswerten Daten der europäischen Nutzer in Europa oder in Ländern mit demselben Datenschutzniveau verbleiben. Wichtig ist auch, ob die Daten über Besucher, Navigation und Verhalten pseudonymisiert und/oder anonymisiert und verschlüsselt werden.

Ausnahmeregelung von der Einwilligung

Die Ausnahmeregelung von der Einwilligung von ePrivacy wird von Datenschutzbehörden wie der CNIL anerkannt. Sie ermöglicht es dem Herausgeber einer Website oder einer mobilen Anwendung, die Notwendigkeit zu umgehen, die vorherige Zustimmung eines Verbrauchers einzuholen, bevor er Tracker (Cookies/mobile ID) hinterlegt. Die Ausnahmeregelung wird nur für Lösungen gewährt, die einen hohen Standard bei der Einhaltung der Datenschutzbestimmungen einhalten und mehrere Bedingungen erfüllen, u.a.:

- Es muss eine generelle Übereinstimmung mit der DSGVO gegeben sein
- Nur Sammlung von Daten, die für die Bereitstellung des vom Benutzer ausdrücklich gewünschten Dienstes unbedingt erforderlich sind
- Für einen Zweck, der sich auf die strikte Messung des Publikums beschränkt

Die Ausnahmeregelung kann nicht nur einen strengeren Datenschutz gewährleisten, sondern auch ein Zeichen für eine bessere Datenqualität sein. Eine Lösung, die die Ausnahmeregelungen für den Datenschutz erfüllt, kann 100"% der Besucherdaten erfassen, während bei Lösungen, die dies nicht tun, nur etwa 50"% der gleichen Daten zugänglich sind.

In-House Expertise

Die DSGVO- und ePrivacy-Gesetzgebung ist nuanciert, und die Art und Weise, wie wir Daten nutzen, verändert sich ständig. Das bedeutet, dass immer die Möglichkeit besteht, dass neue Präzedenzfälle geschaffen werden oder dass weit verbreitete Instrumente wie Privacy Shield (oder was auch immer an dessen Stelle tritt) nicht mehr als legal angesehen werden. Deshalb muss eine Lösung, bei der der Datenschutz im Vordergrund steht, über DSGVO- und ePrivacy-Experten in ihrem Team verfügen, die Erfahrung darin haben, Unternehmen bei der Erfüllung ihrer Datenschutzanforderungen zu unterstützen. Achten Sie auf Kundensupport sowie Daten- und Rechtsexpertise, um sicherzustellen, dass Ihr Anbieter mit den neuen Datenschutzgesetzen Schritt halten kann und Sie dabei unterstützt, auf dem Laufenden zu bleiben.

Datenschutz an erste Stelle stellen

Wenn Sie dem Datenschutz Vorrang vor Kosteneinsparungen einräumen, können Sie sich darauf verlassen, dass Ihr Anbieter mit den Änderungen der Rechtsvorschriften Schritt hält und Sie nicht in den Strudel von Entscheidungen geraten, wie sie in Europa im Jahr 2022 getroffen werden.

Der Wechsel zu einer neuen Lösung bedeutet jedoch, dass Sie Ihre Daten migrieren müssen – ein Schritt, der diese Daten angreifbar machen kann, wenn Sie nicht den richtigen Ansatz wählen. Wie können Sie dies auf sichere Weise tun und gleichzeitig die Datenschutzbedürfnisse Ihrer Kunden respektieren?

Umstellung auf eine neue digitale Analyselösung

Welche nächsten Schritte sind zu beachten, sobald Sie die Entscheidung getroffen haben, auf eine neue digitale Analyselösung umzusteigen? Was ist wirklich erforderlich, um eine neue Lösung in Ihrem Unternehmen einzuführen? Um ein neues Tool schnell zu implementieren, ohne die Daten Ihrer Benutzer zu gefährden, müssen Sie einem bewährten Verfahren folgen.

Diese vier Schritte können Ihnen helfen:

1. Datenmodellierung, Tagging und Dokumentation

Unter Berücksichtigung der ermittelten Geschäftsanforderungen sowie der bereits vorhandenen Berichte, Website-Strukturen, Datenpipelines und Ereignistaxonomien können Sie das für Ihr Unternehmen am besten geeignete Datenmodell festlegen. Ein flexibles Modell ermöglicht es Ihnen, die notwendigen Anpassungen vorzunehmen, wenn sich Ihre Bedürfnisse und Anforderungen im Laufe der Zeit ändern. Wenn Sie sowohl technische Experten als auch Geschäftsanwender in Ihre Analysegespräche einbeziehen, erhalten Sie einen ganzheitlichen Überblick darüber, wonach Sie suchen und wie Analysen und Erkenntnisse in Ihrem gesamten Unternehmen genutzt werden.

Erstellen Sie auf der Grundlage des Datenmodells, für das Sie sich entschieden haben, einen Tagging-Plan, um alle Elemente zu identifizieren, die Sie zur Erreichung Ihrer Kennzahlen benötigen. Um schnell loslegen zu können, sollten Sie einen schrittweisen Tagging-Plan in Betracht ziehen. Standardereignisse wie Seitenaufrufe und Klicks lassen sich in wenigen Stunden implementieren und können in Berichte einfließen, während detailliertere Kennungen im Laufe der Zeit hinzugefügt werden können, wenn Ihre Analyseanforderungen anspruchsvoller werden. Die Analytik sollte ohnehin nie ein Prozess sein, den man einstellt und dann laufen lässt. Mit diesem Ansatz können Sie also sofort einen Wert schaffen und dann im Laufe der Zeit weiter auf Ihrer Grundlage aufbauen.

Wenn Sie Ihr Datenmodell und das Tagging eingerichtet haben, stellen Sie sicher, dass Ihre Dokumentation benutzerfreundliche Beschreibungen der einzelnen Metriken enthält, in denen erklärt wird, welche Informationen ein bestimmter Datensatz enthält.

2. Implementierung

Eine der wichtigsten Komponenten Ihrer Umsetzung ist die Verbindung Ihrer bisherigen Ressourcen – Metriken, Taxonomien usw. – mit Ihrem neuen System. Dies trägt zu einem nahtlosen Übergang für Ihre Endbenutzer bei, da sie Ihr neues System genauso gut verstehen wie Ihr altes. Um dies zu erreichen, sollten Sie einige Dinge beachten:

- Wenn Sie sich für ein Tag Management System (TMS) entscheiden, das in Ihr Analysetool integriert ist, können Sie Ihre bestehende Datenschicht so weit wie möglich nutzen, was den Übergang erleichtert. Ohne ein TMS werden Sie wahrscheinlich zusätzliche Unterstützung durch technische Teams benötigen, was jedoch Ihren Prozess verlangsamen könnte.

- Der gleichzeitige Wechsel aller Tools kann zu Verwirrung in den Teams führen und die Kontinuität Ihrer Berichterstattung beeinträchtigen. Wenn Sie bereits Business-Intelligence-Tools verwenden, wird Ihnen die Wahl einer in diese Plattformen integrierten Analyselösung das Leben erleichtern. Diese Integrationen helfen Ihnen, den Betrieb schneller aufzunehmen, indem sie Daten aus dem neuen System in bestehende Berichte, Dashboards und Visualisierungen einspeisen, die den Anforderungen Ihrer Teams entsprechen.
- Unabhängig davon, welche BI-Tools Sie verwenden, sollten Sie auch alle Berichte berücksichtigen, die in Ihrem bisherigen Analysetool enthalten sind und ersetzt werden müssen. Wenn Sie sich für ein neues Tool entscheiden, das über leistungsstarke, sofort einsatzbereite Berichts- und Datenvisualisierungsfunktionen verfügt, können Sie sofort loslegen, ohne kostbare Zeit mit dem Aufbau und der Anpassung neuer Schnittstellen zu verbringen.

Wenn Ihr neuer Analytik-Anbieter über Onboarding- oder Implementierungsberater verfügt, werden diese Ressourcen in dieser Phase ebenfalls von unschätzbarem Wert für Sie sein, um sicherzustellen, dass Ihre Implementierung mit den gesetzlichen Vorschriften vereinbar ist.

3. Qualitätssicherung und Auditing

Nach der Implementierung sollten Sie eine Reihe von Prüfungen durchführen, um sicherzustellen, dass die Tags korrekt implementiert sind und die Daten wie erwartet auf der Plattform erscheinen. Betrachten Sie dies als eine Art Sicherheitsventil, das dafür sorgt, dass Ihre Daten nicht nach außen dringen.

Bei den meisten Implementierungsprojekten gibt es eine Überschneidungsphase, in der Sie Zugang zu Analysen sowohl für Ihre alte als auch für Ihre neue Lösung haben. Nutzen Sie diese Phase, um die identischen Datensätze in den einzelnen Lösungen zu testen, um zu verstehen, wie sie im Vergleich dastehen und ob Ihre Bereitstellung korrekt erfolgt, und um etwaige Probleme zu erkennen, die Sie beheben müssen.

Je nachdem zwischen welchen Systemen Sie wechseln, kann es zu erwarteten Diskrepanzen zwischen Ihren Datensätzen kommen. Ihr neuer Anbieter sollte Ihnen dabei helfen können, vorherzusagen, wie das aussehen könnte.

4. Schulung und Onboarding

Da alle, von Webanalysten und Produktmanagern bis hin zu Marketingteams, Vertriebsmitarbeitern und Unternehmensmanagern, Ihr digitales Analysetool nutzen, ist die Schulung ein wesentlicher Schritt. Jeder, der die Plattform nutzt, sollte verstehen, wie sie funktioniert, und Zugang zu den Kennzahlen haben, die er braucht, um Entscheidungen zu treffen.

Hier kommt auch Ihre Dokumentation ins Spiel. Wenn Sie Ihre Definitionen in ein zentral verwaltetes Datenmodell einbetten können, hilft das Ihren Teams zu verstehen, worum es geht, und zwar in einer Sprache, die für sie Sinn macht.

Integration von Analytik in Ihr Tagesgeschäft

Sobald sie eingerichtet ist und läuft, kann die digitale Analyse zu einer täglichen Aufgabe werden, da Sie die spezifischen Berichte, Dashboards und Visualisierungen entwickeln, die den Anforderungen Ihrer Geschäftsanwender entsprechen. Ihr Analyseanbieter – sowie alle externen Experten oder Berater, die Sie beschäftigen – sollte in der Lage sein, Ihnen dabei zu helfen, über neue Entwicklungen und Möglichkeiten auf dem Laufenden zu bleiben, um sicherzustellen, dass Sie weiterhin das Beste aus Ihren Daten herausholen und gleichzeitig den gesetzlichen Anforderungen entsprechen.

Wie Piano Analytics helfen kann

Piano Analytics (ehemals Analytics Suite Delta von AT Internet) ist eine digitale Analyselösung, die Funktionen für eine Reihe von Anwendungsfällen bietet, mit einem einheitlichen Datenmodell, das Echtzeitabfragen und 1.400 Ereignisparameter unterstützt. Bei Piano hat der Schutz und die Sicherheit der Nutzerdaten höchste Priorität. Wir haben Maßnahmen ergriffen, die sicherstellen, dass die Nutzerdaten privat bleiben und die Datenschutzgesetze jederzeit eingehalten werden.

Strenge Einhaltung von DSGVO und ePrivacy

Piano Analytics erfüllt die gesetzlichen Anforderungen der DSGVO und von ePrivacy. Wir nutzen einen US-IaaS/Cloud-Anbieter, der den europäischen Verhaltenskodex der Cloud Infrastructure Service Providers (CISPE) befolgt und von der CNIL und dem Europäischen Datenschutzausschuss zugelassen ist.

Strenge Richtlinien für die Datennutzung

Wir erheben nur Daten, die für die Erbringung der vom Kunden definierten und vom Endnutzer ausdrücklich gewünschten Dienstleistung unbedingt erforderlich sind. Der Zweck ist auf die strikte Messung Ihrer Zielgruppe beschränkt, und die Daten gehören immer zu 100"% unseren Kunden.

Ausnahmeregelung von der Einwilligung

Piano Analytics verfügt über eine von der CNIL offiziell anerkannte Ausnahmeregelung, die es dem Herausgeber einer Website, einer mobilen Anwendung oder einer damit verbundenen Plattform erlaubt, vor der Verwendung eines Trackers (Cookie/Mobile ID usw.) nicht ausdrücklich die Zustimmung des Endnutzers/Verbrauchers einzuholen.

In-House Daten-Expertise

Piano hat eine lange Tradition in der Unterstützung von Unternehmen bei der Bewältigung und Einhaltung der sich weiterentwickelnden Datenschutzbestimmungen. Wir sind Experten für DSGVO und ePrivacy und verfügen über umfassende Erfahrung in der Begleitung von Unternehmen bei der Einhaltung von Datenschutzbestimmungen weltweit. Unser Team von Beratern und Datenschutzexperten begleitet unsere Kunden während des gesamten Prozesses der Umsetzung der Ausnahmeregelung von der Einwilligung für die elektronische Datenverarbeitung.

Konfliktfreie Daten

Wir verwenden, verkaufen oder übertragen niemals Daten und führen auch keine Aktivitäten durch, die gegen die DSGVO oder lokale Vorschriften verstoßen würden. Der Standard- und einzige Zweck unserer Lösung ist die Erhebung, Verarbeitung und Speicherung pseudonymisierter Besuchs-, Navigations- und Verhaltensdaten im Namen unserer Kunden. Darüber hinaus ergreifen wir zusätzliche technische Maßnahmen wie Anonymisierung und Verschlüsselung.

Europaweites Vertrauen

Piano ist von Publikumsmessungs-, Daten- und Forschungsagenturen auf dem ganzen Kontinent als anerkannter europäischer Datenanbieter zertifiziert, darunter die Alliance pour les Chiffres de la Presse et des Médias (ACPM) und Médiamétrie in Frankreich, das britische Audit Bureau of Circulation (ABC) und die Stichting KijkOnderzoek (SKO) in den Niederlanden.

Datenschutz steht an erster Stelle

Mit Piano Analytics profitieren Sie von einer fortschrittlichen Analyseplattform, die es Ihnen ermöglicht, hochwertige Daten teamübergreifend zu nutzen, große Datenmengen einfach abzufragen und Ihre Messstrategie an Ihre geschäftlichen Anforderungen anzupassen. Und das alles mit der Gewissheit, dass der Datenschutz bei einer digitalen Analyselösung an erster Stelle steht.

Daten sind für moderne Unternehmen unverzichtbar, und Ihre digitale Analysestrategie ist entscheidend für die Erfüllung der Anforderungen Ihrer Zielgruppe. Aber sich durch die aktuelle Datenschutzlandschaft zu navigieren ist schwieriger als je zuvor – und das digitale Analysetool, für das Sie sich entscheiden, kann den Unterschied zwischen der Einhaltung oder Nichteinhaltung von Vorschriften wie DSGVO und ePrivacy ausmachen.

Die Frage ist: Wie viel Risiko sind Sie bereit einzugehen? Und sind Sie bereit, die schwerwiegenden Konsequenzen einer Nichteinhaltung zu tragen?

Wenn Sie sich für eine digitale Analyselösung entscheiden, bei der der Datenschutz an erster Stelle steht, und Ihre Daten sicher migriert werden, können Sie Besuchsdaten weiterhin in Ihren täglichen Entscheidungsprozess einbeziehen – und dabei gleichzeitig Ihr Risiko minimieren und die sich ständig weiterentwickelnden Datenschutzgesetze einhalten.

Und mit unserer bewährten Expertise kann Piano Analytics Ihnen dabei helfen, dies zu erreichen.