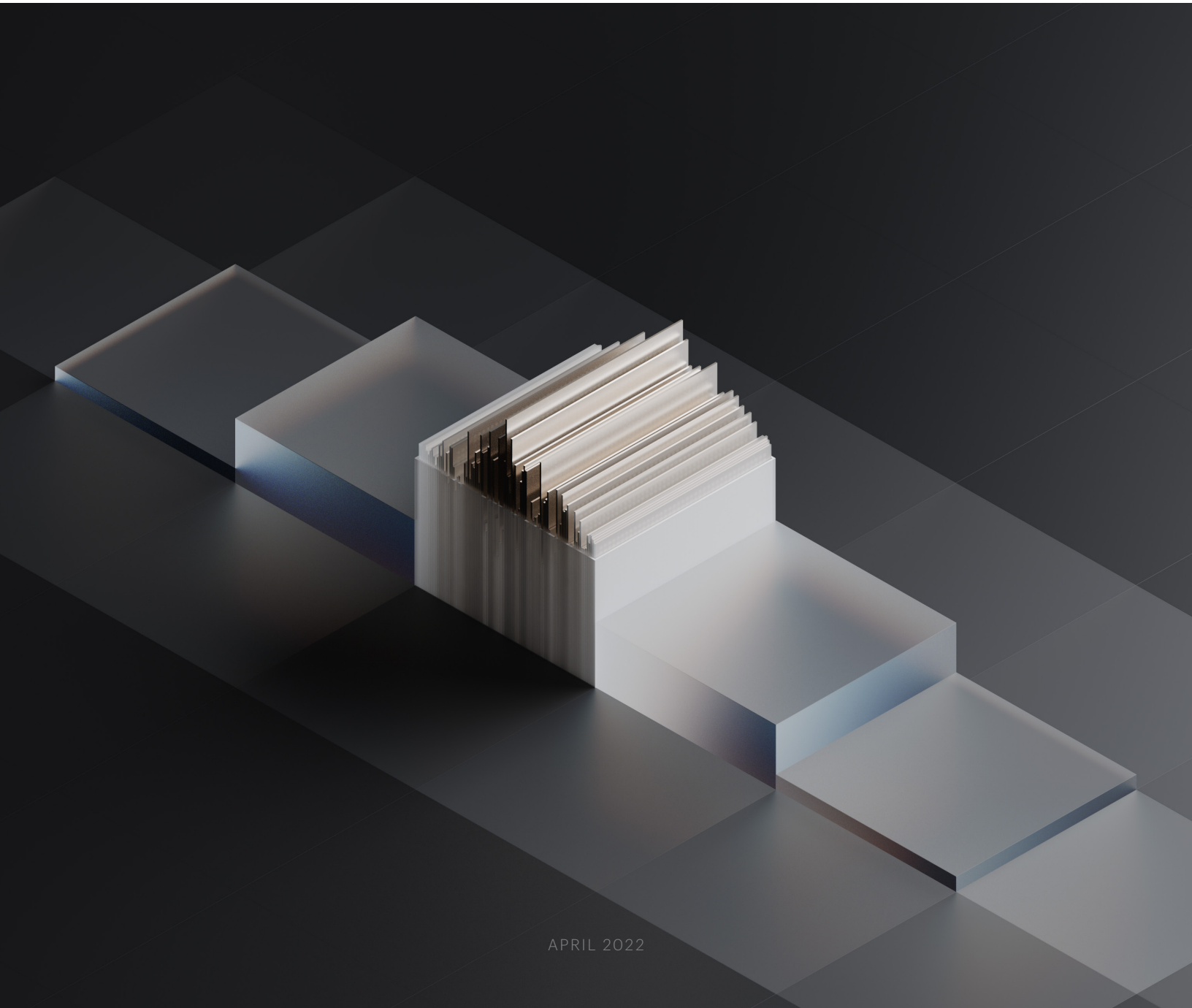
piano analytics

Guide pour une approche centrée sur la confidentialité

Comment élaborer une stratégie Data Analytics conforme à la législation européenne sur la protection de la vie privée ?



APRIL 2022

La protection des données dans le contexte digital moderne est complexe, avec de nouvelles réglementations et normes à respecter.

Ce guide a pour objectif de vous aider à comprendre et à vous repérer dans ce nouvel environnement de travail afin que vous puissiez développer votre activité en toute sérénité.

Décryptage de la confidentialité des données

Le premier véritable signe de changement est apparu en décembre 2021.

C'est à ce moment-là que la Datenschutzbehörde (l'autorité autrichienne de protection des données) s'est prononcée contre la société d'information médicale NetDoktor. L'autorité a jugé que son utilisation de Google Analytics enfreint le règlement général sur la protection des données (RGPD) de l'Union Européenne.

Or, NetDoktor ne faisait aucun usage inhabituel de Google Analytics. Par l'intermédiaire de cookies, la société effectuait un suivi de ses visiteurs sur l'ensemble de son site : pages consultées, temps passé sur le site, etc. Les données relatives à un même utilisateur étaient reliées les unes aux autres au moyen d'un numéro d'identification, ce qui permettait d'obtenir une image plus complète de chaque visiteur. Il existe une multitude d'entreprises, partout dans le monde, qui utilisent cet outil de la même façon.

Comme pour le prouver, la Commission nationale de l'informatique et des libertés (CNIL) de France a prononcé en février 2022 une décision similaire à l'encontre d'une autre société. Le Liechtenstein a annoncé son propre verdict en mars 2022. L'autorité norvégienne de protection des données, Datatilsynet, a conseillé aux organisations de trouver des solutions pour remplacer Google Analytics dans le contexte des enquêtes en cours. De son côté, l'autorité néerlandaise de protection des données (Autoriteit Persoonsgegevens) a fait savoir que l'outil pourrait ne plus être autorisé.

Clairement, le problème ne venait pas de NetDoktor. Ou du moins pas seulement.

Les autorités de protection des données ont toutes convenu que, en autorisant la circulation vers les États-Unis des données des utilisateurs européens sans les garanties adéquates, Google Analytics (et par là-même toutes les entreprises qui l'utilisent) enfreint la réglementation de l'Union européenne en matière de confidentialité des données. Parmi les motifs invoqués, ce type de transfert de données pourrait rendre les données des internautes de l'UE vulnérables aux services de police et d'espionnage américains. Mais que cela signifie-t-il concrètement ? Et quelles en sont les répercussions sur les entreprises qui utilisent le *Digital Analytics* ?

Des effets longue portée

Pour qui s'intéresse aux lois sur la confidentialité des données, les décisions prises en Europe n'ont pas semblé surgir de nulle part.

Tout juste un an et demi auparavant, en juillet 2020, le bouclier de protection des données (ou « Privacy Shield », un ensemble de dispositions fréquemment mis en œuvre pour protéger les données lors de leur transfert entre l'Union européenne et les États-Unis) avait lui-même été jugé illégal par la Cour de justice de l'Union européenne. Or, aucun accord n'avait encore été trouvé pour le remplacer lorsque les arrêts ont commencé à tomber. Selon les responsables européens, la sécurité des données se trouvait ainsi compromise.

À présent, toute entreprise ayant recours à Google Analytics s'expose à un risque de non-conformité – et pas seulement en France, en Autriche ni au Liechtenstein. Il faut s'attendre à une réaction en chaîne.

« Nous anticipons l'adoption progressive de mesures similaires dans la plupart des États membres de l'UE », a déclaré Max Schrems en janvier 2022. Max Schrems est le président honoraire de noyb (None of Your Business), le groupe de défense de la confidentialité des données qui a initialement porté la question des transferts de données devant les autorités européennes. « Nous avons déposé 101 plaintes dans presque tous les États membres, et les autorités ont coordonné leur réponse. »

Or, ces décisions concernent les utilisateurs de Google Analytics non seulement en Europe, mais dans le monde entier. Se trouvent ainsi exposées à un risque de non-conformité toutes les solutions et toutes les entreprises qui exploitent les données de manière similaire.

« Le RGPD s'applique aux sociétés de l'UE ainsi qu'aux entreprises qui traitent des données de citoyens européens, explique Louis-Marie Guérif, DPO du groupe Piano et spécialiste des données en Europe. En somme, à peu près tous ceux qui veulent être présents sur le marché européen et utiliser les données associées doivent respecter le RGPD. »

Ce qui signifie que les entreprises du monde entier ont un choix à faire.

Les implications pour les entreprises

Pour une entreprise qui exploite les données des utilisateurs dans son processus décisionnel (c'est-à-dire la plupart des entreprises aujourd'hui), les récentes évolutions européennes ne sont pas sans effets durables. Sont tout autant concernées les entreprises qui cherchent seulement à connaître le nombre de visiteurs sur leur site ou à savoir quelles sont leurs pages les plus consultées. « C'est une question qui touche tous les aspects de l'économie, tous les aspects de la vie sociale », a déclaré à Wired Gabriela Zanfir-Fortuna, vice-présidente à la protection de la vie privée au niveau mondial au sein du groupe de réflexion à but non lucratif Future of Privacy Forum, en janvier dernier.

C'est toutefois à vous de décider comment réagir. Vous êtes libre de continuer à utiliser Google Analytics, tout en sachant que c'est illégal, dans l'espoir que Google se mettra un jour en conformité (Google a, à date, apporté des changements mineurs qui ont été commentés dans la foulée par l'autorité de contrôle autrichienne et jugée à nouveau insuffisant). Vous pourriez espérer qu'une autre version du bouclier de protection des données ou une solution similaire soit mise en place à court terme, suffisamment solide cette fois pour tenir face aux réglementations européennes. Ou bien vous vous munissez d'une autre solution Digital Analytics qui vous offre les fonctionnalités dont vous avez besoin tout en respectant la législation européenne.

Selon Louis-Marie Guérif, votre réponse dépendra de votre niveau de tolérance au risque. « Ma recommandation, qui est aussi celle des experts, est d'évaluer les risques. Si ce que disent la CNIL et les autres autorités de protection des données vous parle, étudiez les autres options qui s'offrent à vous et trouvez des moyens de réduire le risque. »

Pour évaluer les risques toutefois, vous devez bien comprendre les conséquences possibles de la non-conformité. Or, celles-ci ne s'arrêtent pas aux lourdes amendes infligées. Vous pourriez aller jusqu'à perdre l'accès aux données d'audience que vous avez déjà recueillies en violation de la réglementation.

Ce guide s'adresse à ceux qui évaluent encore les risques encourus et cherchent à appréhender les répercussions possibles en cas de non-respect de la réglementation, ainsi qu'à ceux qui envisagent de changer de solution pour limiter ces risques. Nous examinerons ce qu'il faut prendre en considération pour élaborer une stratégie Digital Analytics axée sur la protection des données, ce qu'il faut rechercher dans une solution qui donne la priorité à la confidentialité et comment migrer vos données en toute sécurité si vous décidez de sauter le pas.

Pour l'instant toutefois, penchons-nous sur la législation dont vous devez tenir compte en matière de protection de la vie privée.

Les lois européennes sur la confidentialité des données

Les décisions récentes nous montrent que les lois européennes sur la confidentialité des données ont le pouvoir de peser sur leur utilisation. Plus strictes que leurs équivalents américains, elles régissent la manière dont votre entreprise collecte, distribue et stocke les données personnelles des utilisateurs européens, qu'elle soit ou non établie en Europe. Il vous sera donc utile de les comprendre si vous utilisez (ou envisagez d'utiliser) une solution Digital Analytics.

Deux fondamentaux encadrent les pratiques relatives aux données en Europe. Examinons-les l'une après l'autre.

Le RGPD

Le règlement général sur la protection des données (RGPD), qui s'inscrit dans le cadre de la législation sur la protection de la vie privée de l'Union européenne, porte, entre autres, sur le transfert de données à caractère personnel en dehors de l'UE et de l'Espace économique européen (EEE). Il stipule que les données ne peuvent être exportées vers des pays qui ne disposent pas d'un « niveau de protection adéquat », c'est-à-dire d'une législation sur la protection des données comparable à celle de l'Europe.

Entré en vigueur en mai 2018, ce règlement exige des entreprises qu'elles fassent preuve de transparence dans leur utilisation des données à caractère personnel. Elles sont ainsi tenues d'informer leurs utilisateurs et clients sur les données qu'elles collectent, de se doter d'une base juridique adéquate pour traiter ces données et de signaler toute violation de données aux personnes concernées. Le RGPD définit les données à caractère personnel comme suit :

Toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une “personne physique identifiable” une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu’un nom, un numéro d’identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale

Sur la base de cette définition, les grandes autorités de protection des données considèrent que les données analytics et les données d’audience constituent des données à caractère personnel et doivent être traitées comme telles : transparence vis-à-vis des utilisateurs sur l’utilisation leurs données, droit d’opposition au traitement ou obligation de protéger ces données de manière appropriée (avec potentiellement des mesures comme la pseudonymisation et l’anonymisation).

La directive ePrivacy

La directive européenne « vie privée et communications électroniques » (dite « directive ePrivacy ») traite des communications électroniques, et notamment de ce que l’on appelle les traceurs : identificateur de cookie, identificateur mobile, pixel, empreinte, etc.

En vertu de cette directive, vous ne pouvez pas lire ni écrire des informations sur le terminal d’un utilisateur final (soit suivre un visiteur ou un utilisateur), à moins d’avoir reçu un consentement préalable adéquat ou de bénéficier d’une exemption spécifique.

La Commission européenne a proposé un nouveau projet de règlement « vie privée et communications électroniques » (dit « règlement ePrivacy ») qui devrait mettre à jour la directive ePrivacy. L’objectif est d’harmoniser totalement le suivi des données et la confidentialité des communications électroniques dans toute l’Europe.

Une portée mondiale

Même si le RGPD et la directive ePrivacy sont des législations européennes, cela ne signifie pas, comme nous l’avons déjà vu, qu’elles concernent uniquement les entreprises de l’UE. Après tout, Internet ne connaît pas de frontières. « Lorsque le RGPD est entré en vigueur, l’un des résultats immédiats a été une augmentation du nombre de sites américains refusant ou restreignant l’accès aux visiteurs européens, a déclaré à Forbes Timo Rein, cofondateur et ancien PDG du fournisseur de CRM Pipedrive, peu après la mise en place du RGPD. Cette approche n’est pas viable. »

Aujourd'hui, toute entreprise possédant un site Web est concernée par le RGPD et la directive ePrivacy, même si elle n'a accès qu'aux données d'audience les plus élémentaires.

Les risques encourus en cas de non-conformité

Toute utilisation des données qui enfreint la directive ePrivacy ou le RGPD peut être lourde de conséquences. En cas de non-conformité avérée, vous risquez un avertissement, des amendes importantes pouvant aller jusqu'à 20 millions d'euros ou 4"% de votre chiffre d'affaires mondial, et une interdiction temporaire ou permanente de traiter des données à caractère personnel. Il peut également vous être demandé de supprimer toutes les données que vous avez déjà collectées en violation de la réglementation.

Si de tels risques vous semblent inacceptables, vous devez avant tout élaborer une stratégie bien pensée de gestion des données. Point tout aussi essentiel, il vous faudra trouver un fournisseur Digital Analytics qui comprenne le RGPD et la directive ePrivacy, et qui dispose de l'expertise nécessaire pour rester au fait des exigences législatives.

L'élaboration d'une stratégie de confidentialité des données

La plupart des entreprises comprennent aujourd'hui l'importance du Digital Analytics. L'analyse du comportement des internautes vous permet de faire de meilleurs choix stratégiques en fonction des besoins de votre audience et de créer une expérience utilisateur optimale – à condition bien sûr de disposer de données de qualité. Mais si vous voulez déjouer les pièges potentiels, préserver la confiance de vos utilisateurs et continuer à vous frayer un chemin praticable dans le paysage réglementaire, vous avez également besoin d'une stratégie à long terme en matière de confidentialité des données, quelle qu'en soit la forme.

« Discutez avec les responsables de la protection des données et le service juridique de votre entreprise, ainsi qu'avec toutes vos équipes qui traitent des données», suggère Louis-Marie Guérif. « Ne vous contentez pas de prendre une décision rapide que vous paierez potentiellement dans six ou douze mois. La protection de la vie privée est une affaire de gestion du risque : vous devez peser le risque de recevoir une amende, de perdre des données ou de ne pas pouvoir exploiter vos données. »

Pour donner la priorité à la conformité sur le long terme, il importe néanmoins de savoir quoi rechercher dans une solution *Digital Analytics*.

Déceler les coûts cachés de la gratuité

Malgré le rôle essentiel joué par le Digital Analytics, de nombreuses entreprises continuent de choisir leur solution selon des critères de réduction des dépenses plutôt que sur la base des fonctionnalités proposées. Or, comme on le constate actuellement en Europe, la gratuité d'une solution cache différents coûts, qui ne sont pas sans conséquences pour la vie privée des utilisateurs.

Pour bien comprendre ces coûts cachés, nous allons examiner les deux types de solutions Digital Analytics gratuites disponibles sur le marché.

Les solutions open source locales

Les solutions *Digital Analytics* open source et locales sont les moins courantes des solutions gratuites disponibles. Et pour cause : elles ne fournissent pas les données complexes dont les entreprises ont aujourd'hui besoin sur leurs utilisateurs. Qui plus est, de telles solutions vous confient toute la responsabilité en matière de sécurité et de protection de la vie privée.

Il vous appartient donc de suivre les évolutions du RGPD, de la directive ePrivacy et, plus généralement, de tout le paysage de la confidentialité des données. À vous également d'adapter votre utilisation en fonction des dispositions réglementaires. Si vous ne disposez pas des ressources ou des compétences nécessaires pour rester à la page, vous prenez le risque de vous retrouver en dehors des clous.

Le prix à payer pour recueillir des données

Les solutions gratuites les plus courantes sont, bien sûr, les solutions du type Google Analytics. Elles fournissent des données d'audience plus avancées, mais il y a un « mais ». « Le problème avec la gratuité, c'est que vous êtes le produit, en tant qu'utilisateur », explique Louis-Marie Guérif.

Le prix à payer réside dans les données clients que vous collectez : elles peuvent être exploitées à des fins qui échappent à votre contrôle (profilage des utilisateurs, publicité numérique) sans le consentement des utilisateurs. Il peut par ailleurs être difficile pour ces derniers de refuser le suivi des données et de gérer la manière dont elles sont employées. De plus, rares sont les fournisseurs de solutions gratuites qui vous aident, grâce à une assistance et à des ressources spécialisées, à vous mettre en conformité avec les exigences réglementaires du RGPD et de la directive ePrivacy.

« Il est courant que les petites solutions et les solutions gratuites ne comptent pas d'experts à qui vous pouvez vous adresser pour configurer votre solution dans le respect de la réglementation», explique Louis-Marie Guérif. « Vous devez plus ou moins vous débrouiller par vous-même. »

Trouver une solution analytics respectueuse de la confidentialité

Si toutefois la gratuité n'est pas votre priorité, vous pouvez choisir une solution qui intègre toutes les fonctionnalités et tous les types de données dont vous avez besoin, et placer par là-même la confidentialité des données en tête de votre liste.

Pour trouver une solution Digital Analytics respectueuse de la confidentialité, prenez d'abord en compte les points suivants.

La définition des « données à caractère personnel »

Rappelez-vous la manière dont le RGPD définit les « données à caractère personnel ». Si vous voulez une solution qui reste en règle, vous devez vous tourner vers un fournisseur qui emploie la même définition, et place notamment dans cette catégorie les cookies, identificateurs mobiles et autres adresses IP. Une solution qui ne désigne pas les données personnelles de la même manière risque de devenir non conforme.

L'utilisation et le stockage des données

Les décisions prises dans l'Union européenne portent essentiellement sur le lieu de stockage des données et la manière dont elles sont exploitées. En vertu du RGPD, les données privées des utilisateurs européens doivent rester en Europe ou dans des pays offrant le même niveau de protection des données. Il est également important de vérifier si les données des internautes (audience, navigation et comportement) sont pseudonymisées ou anonymisées, et si elles sont chiffrées.

La dispense de consentement

La dispense de consentement ePrivacy est reconnue par différentes autorités de protection des données, notamment en France (CNIL), mais aussi en Allemagne, au Royaume-Uni, en Italie et dans plusieurs autres pays de l'UE. Elle permet à un éditeur de site ou d'application mobile de ne pas avoir à demander le consentement d'un utilisateur avant de déposer des traceurs (cookies et identificateurs mobiles). Cette exemption n'est accordée qu'aux solutions qui maintiennent un niveau élevé de confidentialité et qui remplissent plusieurs conditions :

- Conformité générale au RGPD
- Collecte des données strictement nécessaires à la prestation de service demandée par l'utilisateur (et d'aucune autre donnée)
- Finalité limitée à la seule mesure de l'audience

Une approche centrée sur la confidentialité des données

Outre la garantie d'une protection plus rigoureuse de la vie privée, la dispense de consentement peut également être le signe d'une meilleure qualité des données. Une solution conforme aux critères d'exemption ePrivacy peut collecter 100"% des données d'audience, contre environ 50"% pour les autres solutions.

L'expertise en interne

Le RGPD et la directive ePrivacy sont des réglementations subtiles, et les usages des données évoluent en permanence. Il est toujours possible qu'un nouveau précédent soit établi ou que des dispositions largement appliquées comme le bouclier de protection des données (ou son successeur) ne soient plus d'actualité. C'est pourquoi un fournisseur de solution axé sur la confidentialité doit compter dans son équipe des experts du RGPD et de la directive ePrivacy. Il doit posséder l'expérience nécessaire pour guider les entreprises dans leur démarche de protection des données. Veillez également à ce qu'il mette à votre disposition une assistance à la clientèle et des spécialistes des données et du droit : autant de prérequis essentiels qui vous permettront de rester en phase avec la législation.

Donner la priorité à la confidentialité des données

En privilégiant la protection de la vie privée plutôt que la réduction de vos dépenses, vous vous assurez de pouvoir compter sur votre fournisseur. En effet, celui-ci restera au fait des évolutions réglementaires, ce qui vous évitera de vous retrouver aux prises avec des décisions comme celles que l'on voit fleurir cette année en Europe.

Mais adopter une nouvelle solution signifie migrer vos données : une étape qui, à défaut d'une approche adéquate, peut les rendre vulnérables. La question qui se pose donc est la suivante : comment passer à un nouveau fournisseur tout en respectant les impératifs de confidentialité de vos clients ?

La migration vers une nouvelle solution Digital Analytics

Que faire une fois que vous avez pris la décision de migrer vers une autre solution Digital Analytics ? Quelles sont les conditions nécessaires à la mise en œuvre d'un nouvel outil au sein de votre entreprise ? Et, surtout, comment procéder à ce changement rapidement sans compromettre les données de vos utilisateurs ? Nous vous recommandons pour cela de suivre un processus en quatre étapes :

1. La modélisation, le marquage et la documentation des données

Déterminez le modèle de données qui servira au mieux les besoins de votre entreprise, en gardant à l'esprit les rapports, la structure du site, le pipeline de données et la taxonomie des événements que vous avez déjà mis en place. Un modèle flexible vous permettra d'apporter les ajustements nécessaires au fil de l'évolution de vos exigences. Impliquez à la fois des experts techniques et des utilisateurs professionnels dans votre réflexion sur l'analytics. Vous pourrez ainsi brosser une vue d'ensemble de vos besoins ainsi que de votre usage actuel de l'analytics et des informations à travers toute l'entreprise.

Sur la base du modèle de données choisi, créez un plan de marquage afin d'identifier tous les éléments nécessaires à vos indicateurs. Pour un démarrage plus rapide, adoptez un plan de marquage progressif. Les événements standard (par exemple les pages vues et les clics) peuvent être mis en œuvre en quelques heures pour produire aussitôt des rapports. Ajoutez ensuite un marquage plus détaillé au fur et à mesure que vos besoins d'analytics s'affinent. L'analytics ne doit de toute façon jamais être un processus figé. Cette approche vous permettra donc de dégager une valeur immédiate, puis de continuer à consolider vos bases au fil du temps.

Une fois votre modèle de données et votre marquage en place, documentez vos indicateurs d'une manière qui soit compréhensible par tous (y compris des non-spécialistes), en détaillant les informations contenues dans chaque donnée.

2. La mise en œuvre

L'un des aspects les plus déterminants du processus d'implémentation consiste à relier vos anciennes ressources (indicateurs, taxonomies, etc.) à votre nouveau système. L'objectif est de rendre la transition aussi transparente que possible pour vos utilisateurs finaux. Ces derniers doivent en effet conserver le même niveau de maîtrise malgré le changement de système. Voici quelques conseils pour y parvenir :

- Choisissez un système de gestion de balises (TMS, pour « Tag Management System ») compatible avec votre solution analytics. Vous pourrez ainsi tirer pleinement parti de votre couche de données déjà en place de façon à faciliter la transition. Sans TMS, vous aurez probablement besoin de faire davantage appel aux équipes techniques, ce qui risquerait de ralentir le processus.

- Un changement simultané de toutes les solutions peut être source de confusion parmi les équipes et nuire à la continuité de vos rapports. Si vous utilisez déjà des outils d'informatique décisionnelle, vous vous faciliterez la vie en choisissant une solution analytics compatible. Ces intégrations vous aideront même à vous lancer plus rapidement : vous pourrez introduire les données du nouveau système dans les rapports, tableaux de bord et visualisations qui répondent déjà aux besoins de vos équipes.

- Quels que soient les outils d'informatique décisionnelle que vous utilisez, tenez également compte des éventuels rapports natifs de votre ancienne solution analytics que vous devrez remplacer. En choisissant une nouvelle solution dotée de solides fonctions de reporting et de visualisation des données prêtes à l'emploi, vous pourrez passer tout de suite à l'action. Cela vous évitera de perdre un temps précieux à construire et à personnaliser de nouvelles interfaces.

Certains fournisseurs de services analytics mettent à votre disposition des consultants chargés de l'intégration ou de la mise en œuvre : autant de ressources qui à ce stade vous seront également d'une grande aide pour garantir une implémentation conforme à la réglementation.

3. L'assurance qualité et les audits

Mettez en place une série de contrôles pour vérifier que les tags sont correctement mis en œuvre et que les données qui apparaissent dans la solution sont conformes à vos attentes. C'est cette soupape de sécurité qui vous évitera des fuites de données.

La plupart des projets d'implémentation prévoient une période de chevauchement entre l'ancienne et la nouvelle solution analytics. Profitez de cette étape pour comparer les ensembles de données de part et d'autre et, le cas échéant, analyser leurs différences. C'est également le moment de vérifier que tout est bien en place et d'identifier d'éventuels problèmes à résoudre.

En fonction des systèmes concernés, des divergences peuvent être attendues ; votre nouveau fournisseur devrait toutefois être en mesure de vous aider à les anticiper.

4. La formation et la mise en route

Analystes Web, chefs de produit, spécialistes marketing, commerciaux ou encore dirigeants : compte tenu du large panel d'utilisateurs de votre solution Digital Analytics, le volet formation constitue une étape à part entière. Chacune de ces parties prenantes doit comprendre son fonctionnement et avoir accès aux indicateurs dont elle a besoin pour prendre ses décisions.

L'intégration de l'analytics dans votre travail quotidien

Une fois votre système en place et opérationnel, le Digital Analytics peut devenir une activité de routine pour vos collaborateurs grâce aux rapports, tableaux de bord et visualisations que vous développez spécifiquement pour répondre à leurs besoins. Votre fournisseur analytics (de même que les experts et consultants externes auxquels vous faites éventuellement appel) doit pouvoir vous aider à suivre les nouveaux développements et à saisir les nouvelles occasions, dans un double objectif : d'une part, tirer le meilleur parti de vos données et, d'autre part, rester en phase avec les exigences réglementaires.

Piano Analytics au service de votre entreprise

Piano Analytics (anciennement Analytics Suite Delta d'AT Internet) est une solution Digital Analytics qui offre des fonctionnalités pour toute une série de cas d'utilisation, avec un modèle de données unifié prenant en charge les requêtes en temps réel ainsi que 1 400 paramètres d'événements. La protection de la vie privée et la sécurité des données des utilisateurs figurent en tête de nos priorités. Nous avons ainsi mis en place des mesures visant à préserver la confidentialité des données et à garantir en permanence le respect de la législation.

Une conformité stricte au RGPD et à la directive ePrivacy

Piano Analytics se conforme aux exigences réglementaires prévues par le RGPD et la directive ePrivacy. Nous faisons appel à un fournisseur américain IaaS et cloud qui respecte le code de conduite européen soumis par l'association CISPE (Cloud Infrastructure Services Providers in Europe), approuvé par la CNIL et le Conseil européen de la protection des données.

Des politiques rigoureuses en matière d'utilisation des données

Nous ne collectons que les données strictement nécessaires à la prestation de service définie par nos clients et expressément demandée par l'utilisateur final. La finalité est limitée à la seule mesure de votre audience. Nos clients restent par ailleurs propriétaires à 100"% de leurs données.

La dispense de consentement

Piano Analytics dispose d'une exemption au recueil du consentement reconnue officiellement par la CNIL. Elle dispense l'éditeur d'un site Web, d'une application mobile ou d'une solution connectée de recueillir expressément le consentement de l'utilisateur final avant d'utiliser un traceur (cookie, identificateur mobile, etc.).

Cette exemption peut être invoquée dans tous les pays européens où a été transposée la directive ePrivacy.

Une expertise interne en matière de données

Piano aide depuis longtemps les entreprises à se familiariser avec les réglementations relatives à la protection des données et à s'adapter à leur évolution. En notre qualité d'experts du RGPD et de la directive ePrivacy, nous possédons une grande expérience dans l'accompagnement des sociétés au travers des différentes dispositions légales en vigueur dans le monde entier. Notre équipe de consultants et de spécialistes de la confidentialité assiste nos clients tout au long du processus de mise en œuvre de l'exemption ePrivacy et de mobilisation de leurs données.

Des données exemptes de tout conflit d'intérêts

Nous n'exploitons, ne vendons ni ne transférons jamais de données. Plus généralement, nous ne nous livrons à aucune activité susceptible d'enfreindre le RGPD et les réglementations locales. L'unique objectif de notre solution consiste à collecter, à traiter et à stocker différentes données pseudonymisées (audience, navigation et comportement) pour le compte de nos clients. Nous avons également mis en place des mesures techniques supplémentaires, notamment l'anonymisation et le chiffrement.

Un fournisseur reconnu dans toute l'Europe

En tant que fournisseur de données européen, Piano est certifié et approuvé par des organismes de mesure d'audience, de contrôle des données et de recherche de tout le continent, notamment l'ACPM (Alliance pour les chiffres de la presse et des médias) et Médiamétrie en France, ABC (Audit Bureau of Circulations) au Royaume-Uni et SKO (Stichting KijkOnderzoek) aux Pays-Bas.

La confidentialité avant tout

Piano Analytics est une solution analytics avancée qui vous permet de partager des données de qualité avec les différents collaborateurs de l'entreprise, d'interroger facilement de grands volumes de données et de personnaliser votre stratégie de mesure en fonction des besoins de votre entreprise. Le tout avec la tranquillité d'esprit que procure une solution Digital Analytics 100"% axée sur la confidentialité..

Les données font partie intégrante de toute entreprise moderne, et votre stratégie Digital Analytics est essentielle pour répondre aux besoins de votre audience. Cependant, le paysage actuel de la confidentialité des données est plus difficile à appréhender que jamais. La solution Digital Analytics que vous choisissez d'utiliser peut faire toute la différence entre conformité et non-conformité vis-à-vis de réglementations telles que le RGPD et la directive ePrivacy.

La question est donc : dans quelle mesure acceptez-vous de prendre des risques ? Êtes-vous capable d'assumer les lourdes conséquences du non-respect de la réglementation ?

En migrant vos données de manière sécurisée vers une solution Digital Analytics qui accorde la priorité à la protection de la vie privée, vous pourrez continuer à intégrer vos données d'audience dans votre processus décisionnel. Vous limiterez également les risques encourus et resterez en règle au regard des lois sur la protection de la vie privée, qui ne cessent d'évoluer.

Piano met à votre service son expertise reconnue pour vous aider à y parvenir.

Pour en savoir plus sur la solution analytics de Piano, 100"% axée sur la confidentialité, contactez-nous à l'adresse hello@piano.io.

Piano Analytics vous aide a comprendre et interpréter vos données analytics tout en restant conforme aux réglementations les plus strictes sur la sécurité et la protection des données.

Visitez piano.io pour demander une démo.

piano ANALYTICS + ACTIVATION

La plateforme de *digital experience* de Piano aide les entreprises à comprendre et à monétiser leur audience. Grâce à la centralisation des données clients, à l'analyse des indicateurs comportementaux et à la création de parcours clients personnalisés, notre solution permet aux marques d'accélérer le lancement de leurs campagnes et produits. Elle met à votre disposition tous les outils nécessaires pour renforcer l'engagement de vos clients et développer une personnalisation à grande échelle. Nous comptons parmi nos clients des entreprises dans le monde entier, notamment Air France, la BBC, CBS, IBM, Kirin Holdings, Jaguar Land Rover, Nielsen et le Wall Street Journal. Notre société a été reconnue comme l'une des entreprises technologiques innovantes à la croissance la plus rapide au monde par le Forum économique mondial, Deloitte, American City Business Journals et d'autres encore. Pour en savoir plus, rendez-vous sur piano.io.