RGPD : une évolution, pas une révolution

Mentions légales
Cet article ne constitue pas une consultation juridique, et n'est pas destiné à créer ni susciter une relation entre un client et son avocat. Demandez conseil à un professionnel du droit si nécessaire.

Introduction

Le RGPD (Règlement Général pour la Protection des Données) remplace la directive sur la protection des données personnelles adoptée en 1995, et harmonise les différentes lois relatives à la protection des données des 28 États membres de l'Union européenne.

Depuis notre création en 2005, nous avons toujours œuvré pour que notre technologie soit à la pointe de la sécurité et de la protection de la vie privée, tout en répondant aux attentes de nos clients grâce à des annonces publicitaires personnalisées et pertinentes. Criteo est une entreprise internationale avec d'importantes représentations dans plusieurs pays de l'UE, et des partenariats avec des milliers d'annonceurs et d'éditeurs dont les clients et utilisateurs sont basés en Europe. Dans ce contexte, nous sommes habitués à nous conformer aux exigences locales en matière de protection de la vie privée, comme nous le faisons partout dans le monde.

Chez Criteo, nous pensons que la transparence et la confiance autour de la confidentialité et de la protection des données servent les entreprises comme leurs clients. C'est pourquoi nous nous engageons à respecter les normes imposées par le RGPD, et à collaborer avec les clients et partenaires soumis à cette nouvelle réglementation, en leur apportant notre soutien et en partageant les bonnes pratiques nécessaires pour une transition en toute simplicité. Parce que nous sommes prêts à relever le défi du RGPD, nous anticipons un impact relativement faible sur la capacité de nos clients et partenaires à utiliser nos solutions.

De manière générale, cette réforme est une évolution qui harmonise les règles en matière de protection des données dans les États membres de l'UE, tout en offrant une application homogènes par les Autorités de protection des données (DPA) dans chaque État membre. Les objectifs du RGPD sont clairs :

- Moderniser le système juridique pour protéger les données personnelles dans une ère de mondialisation et d'innovation technologique.
- Renforcer les droits des individus tout en réduisant la charge administrative sur les entreprises et assurer une libre circulation des données personnelles au sein de l'UE.

- Apporter clarté et cohérence aux règles relatives à la protection des données personnelles et veiller à une application homogène et une mise en œuvre efficace dans toute l'UE.

Comment le RGPD définit-il la notion de « donnée personnelle » ?

Le RGPD protège la vie privée des citoyens de l'UE et s'applique à toutes les entreprises recueillant ou traitant des données personnelles sur les individus au sein de l'UE, qu'elles soient ou non implantées dans un État membre de l'UE. Dans le cas du marketing digital, le RGPD s'applique à toutes les informations concernant une personne physique identifiable ou identifiée, ce qui comprend les technologies de suivi publicitaire telles que les cookies ou les identifiants publicitaires mobiles (Mobile Advertising IDs). Ces identifiants sont désormais couverts par la définition des données personnelles, reflétant l'interprétation globale des données personnelles déjà présente dans les lois européennes.

Il est important de souligner que ces identifiants étaient déjà considérés comme des données personnelles par de nombreuses DPA européennes. Pour Criteo, qui ne collecte que ce type de données personnelles non sensibles par le biais de cookies, ce principe s'inscrit dans la continuité de nos pratiques. Nous sommes familiers de cette distinction, et appliquons déjà les méthodes conformes à ces exigences tout en offrant un service de qualité à nos clients.

Nous savons que les entreprises se posent de nombreuses questions sur les conséquences en matière de gestion des données. Commençons donc par le commencement : que signifie la notion de « donnée personnelle » au sens du RGPD ? Pour la nouvelle loi, est considérée comme donnée personnelle :

- *Tout ce qui permet d'identifier directement une personne* : prénom, nom, numéro de téléphone etc.
- *Toute donnée «* pseudonymisée*» ou donnée indirectement identifiante*, c'est-à-dire ne permettant pas directement d'identifier une personne, mais permettant d'isoler des comportements individuels (par exemple dans le but de diffuser les bonnes publicités au bon utilisateur, au bon moment).

Le RGPD établit une distinction claire entre les informations directement identifiantes et les informations pseudonymisées. Il encourage l'utilisation de données pseudonymisées et prévoit expressément que « *La pseudonymisation des données à caractère personnel peut réduire les risques pour les personnes concernées et aider les responsables du traitement et les sous-traitants à remplir leurs obligations en matière de protection des données*. »[1].

Les données recueillies et traitées par Criteo pour ses clients et partenaires ne sont pas considérées comme « sensibles » au sens du RGPD. Alors quelles données le sont ? Les données sensibles sont toutes les données susceptibles de révéler :

- l' origine raciale ou ethnique
- Les opinions politiques

[1] *Règlement Général sur la Protection des Données – considérant 28*

- Les convictions religieuses ou philosophiques
- l'appartenance syndicale
- Des données génétiques
- Des données biométriques aux fins d'identifier une personne
- Des données concernant la santé, l'orientation ou la vie sexuelle d'une personne

Criteo, pour sa part, ne recueille que les données techniques pseudonymisées liées aux évènements de navigation. Lorsqu'ils travaillent avec Criteo, ses clients et partenaires n'ont besoin que de données pseudonymisées qui ne permettent pas l'identification directe des utilisateurs. Ces données pseudonymisées comprennent :

- Les identifiants cookies
- Les adresses email hachées
- Les identifiants de publicité mobile
- Tout autre identifiant technique qui permet à Criteo de distinguer un comportement individuel sans directement identifier un individu

Quelle est la différence entre le consentement non ambigu et le consentement explicite ?

Le RGPD établit aussi une distinction claire entre le consentement non ambigu et le consentement explicite d'un individu. Si les deux formes de consentement impliquent une action positive de la part de l'utilisateur, le consentement explicite, lui, impliquera une interprétation stricte de ce que doit être cette action (ex : cocher une case, cliquer sur un bouton « J'accepte »). Ceci s'applique aux données personnelles sensibles telles que l'origine raciale, la religion, l'orientation sexuelle, l'affiliation politique et la santé. Isolément, les identifiants techniques (les cookies, par exemple) doivent être considérés comme des données personnelles non sensibles pour la collecte desquelles le consentement explicite n'est pas nécessaire la seule base légale disponible

Alors que cela signifie-t-il, et comment cela s'applique-t-il à votre entreprise ? Le RGPD prévoit six bases légales distinctes pour collecter et traiter des données personnelles en Europe. Ainsi, quelles que soient les données personnelles concernées, leur collecte doit être fondée sur une base légale. Ces six bases légales sont :

- L'intérêt vital de la personne
- L'intérêt public
- La nécessité contractuelle
- Le respect d'obligations légales
- Le consentement non-ambigu de la personne
- L'intérêt légitime du responsable de traitement

Il est important de noter que ces six bases légales ont une valeur juridique équivalente et ne sont pas cumulatives – autrement dit, une seule suffit à justifier un traitement. Pour les entreprises dans le domaine du marketing ou du marketing digital, ou pour celles qui recueillent des données pour une finalité de marketing, les deux bases légales les plus pertinentes sont : (1) le consentement non-ambigu de la personne et (2) l'intérêt légitime du responsable de traitement.

Nous pensons que le consentement non-ambigu est la base légale la plus pertinente pour nos clients et partenaires collectant des données personnelles en ligne, notamment par le biais de cookies ou d'identifiants techniques similaires.

En Europe, le consentement pour les cookies de retargeting est appliqué depuis 2009, avec l'adoption de la directive ePrivacy (ou « directive cookie »). Les clients et éditeurs partenaires de Criteo qui ne collectent pas de données sensibles, et se basent uniquement sur des identifiants techniques pseudonymisés associés à la navigation, aux intentions et historiques d'achats, respectent déjà ces règles.

Pour Criteo, les nouvelles règles autour du consentement non-ambigu s'inscrivent dans la continuité des lois protectrices déjà appliquées en Europe. La CNIL (Commission nationale de l'informatique et des libertés) recommande elle-même ces pratiques, et suggère plusieurs solutions techniques simples aux administrateurs de sites Web.

Les critères requis par le RGPD pour définir un consentement non-ambigu valide sont très similaires, sinon identiques, aux critères déjà détaillés par le Groupe de Travail de l'Article 29 (G29) dans un précédent rapport[2] :

> ***Informations spécifiques :*** *« Pour être valable, le consentement doit être spécifique et fondé sur des informations appropriées. En d'autres termes, un consentement général, sans préciser la finalité exacte du traitement, n'est pas acceptable. »*
>
> ***Moment où le consentement est donné :*** *« De manière générale, le consentement doit être exprimé avant le début du traitement. »*
>
> ***Choix actif :*** *« Le consentement doit être indubitable. Dès lors, la procédure relative à l'obtention et à l'octroi du consentement ne doit laisser aucun doute quant à l'intention de la personne concernée. En principe, il n'existe pas de limitations quant à la forme que peut revêtir un consentement. Toutefois, pour être valable, le consentement doit consister en une manifestation active de la volonté de l'utilisateur. L'expression minimale d'une manifestation de volonté pourrait être tout type de signe, suffisamment clair pour permettre d'exprimer la volonté d'une personne concernée et être compris par le responsable du traitement. »*
>
> ***Libre manifestation de volonté :*** *« Le consentement ne peut être valable que si la personne concernée est véritablement en mesure d'exercer un choix et s'il n'y a pas de risque de tromperie, d'intimidation, de coercition ou de conséquences négatives importantes si elle ne donne pas son consentement. »*

[2] *Le Groupe de Travail de l'Article 29 – Document de travail n° 02/2013 énonçant des lignes directrices sur le recueil du consentement pour le dépôt de cookies: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf*

Comment s'applique « l'intérêt légitime du responsable de traitement » ?

Afin que le traitement des données soit considéré comme dans l'intérêt légitime, les utilisateurs doivent s'attendre raisonnablement à ce qu'un tel traitement soit réalisé avec leurs données. Un traitement de données à des fins de marketing direct pourrait être considéré et réalisé dans le cadre de l'intérêt légitime. Cependant, cet intérêt légitime ne doit pas outrepasser les droits fondamentaux à la vie privée des utilisateurs, et des mesures de sécurité appropriées doivent être mises en œuvre afin de réduire les risques potentiels pour les données.

En tout état de cause, les principes de base à respecter avant de se fonder sur l'intérêt légitime sont les suivants :

- Une explication complète de la nature des données collectées, la finalité précise de cette collecte, ainsi que la façon dont cela impacte l'expérience de navigation pour l'utilisateur. Exemple :

  « Notre [site/application] utilise des cookies/des identifiants publicitaires à des fins de publicité personnalisée. Ces technologies de ciblage publicitaire nous permettent d'afficher des publicités aux internautes intéressés par nos produits sur des sites web et applications partenaires. Nos technologies de retargeting utilisent vos cookies ou vos identifiants publicitaires pour afficher des annonces basées sur votre historique de navigation. Pour en savoir plus et/ou vous opposer à ces services, merci de vous référer à la politique de confidentialité listée ci-dessous. » [Ajoutez le lien vers la politique de confidentialité de votre partenaire, autrement dit celle de Criteo à l'adresse : http://www.criteo.com/fr/privacy/]

- Un moyen pour les utilisateurs de contrôler leur expérience, notamment de pouvoir se désinscrire, simple à utiliser et aisément accessible, expliquant la façon dont cela affecte leur expérience.
- Un accès simple à la politique de confidentialité, ainsi qu'aux informations sur les normes de protection de la vie privée auxquelles sont soumises les entreprises du secteur, ou sur les engagements pris par votre entreprise. Exemple : Criteo est membre de la Network Advertising Initiative.

Les entreprises doivent se poser les questions clés avant de se fonder sur l'intérêt légitime, notamment :

- À quelle fin les données sont-elles recueillies ?
- La collecte est-elle nécessaire afin de répondre à un ou plusieurs objectifs spécifiques de l'entreprise ?
- Le RGPD ou d'autres lois nationales identifient-ils spécifiquement la finalité du traitement comme étant une activité légitime, sous réserve de la réalisation d'une analyse d'impact sur la vie privée des individus et d'un résultat positif ?
- Existe-t-il un autre moyen de réaliser cette finalité ?
- La personne s'attend-elle à ce que ce traitement ait lieu ?

- Quelle est la nature des données à traiter ? Est-ce que la nature de ces données bénéficie d'une protection spécifique dans le cadre du RGPD ?
- Ce traitement limiterait-il ou fragiliserait-il les droits des individus ?
- Une information claire est-elle délivrée à la personne ? Si oui, comment ? Est-elle suffisamment compréhensible et claire quant aux objectifs du traitement ?

Quelle est l'approche de Criteo en matière de confidentialité des données ?

Chez Criteo, la confidentialité des données personnelles est une priorité. Nous nous efforçons de protéger et de traiter les données dans le respect des règles relatives à la protection et la confidentialité des données - y compris celles imposées par le RGPD.

La confidentialité est au cœur de chaque fonctionnalité développée par nos équipes produits - elle est le principe fondateur de « Privacy by Design », une approche sophistiquée garantissant les meilleures pratiques de sécurité du secteur, pour les annonceurs comme les consommateurs.

« Privacy by Design », c'est l'engagement de longue date de notre entreprise pour une industrie capable d'assurer la confidentialité et la sécurité des données. En voici les principes fondamentaux :

- Comme exigé par le RGPD, nous avons désigné un Data Privacy Officer depuis 2013, épaulé par une équipe d'experts en protection et confidentialité des données.
- Ces experts sont rattachés aux équipes Product et R&D. Ils effectuent des contrôles systématiques et continus, de manière à surveiller les risques potentiels tout au long du cycle de vie de nos produits, et à réduire ces risques de manière proactive.
- L'équipe Data Privacy dispense de nombreuses formations à l'échelle de l'entreprise, fait appliquer les codes de conduite et contribue à créer les meilleurs produits et services.
- Nous révisons et documentons régulièrement nos politiques internes, modifions nos politiques de confidentialité existantes si nécessaire et faisons appliquer ces politiques par nos partenaires et vendeurs.

Des mesures de sécurité sans compromis

Comme l'exige le RGPD, nous respections déjà des mesures de sécurité extrêmement strictes en ce qui concerne la collecte des données de nos clients. Nous utilisons des méthodes de pseudonymisation modernes, notamment les fonctions de hachage double MD5 et SHA-256, reconnues comme les plus fiables et efficaces dans le cadre du RGPD. Nous ne stockons jamais les informations d'identification directes des consommateurs de façon volontaire. Pour des questions de conformité et d'optimisation des performances, nous stockons les données des consommateurs européens au sein du data center européen le plus proche d'eux.

Ad Choices : le point sur les droits et le contrôle des consommateurs

Criteo reconnaît depuis longtemps l'importance de l'équilibre entre la pertinence des publicités, le respect de la vie privée des consommateurs et leur besoin de se sentir aux commandes de leur expérience. Et les consommateurs ont bien saisi cette subtilité. C'est pourquoi Criteo s'est engagé dans le programme Ad Choices dès 2008, pour permettre aux consommateurs, en un simple clic, de savoir exactement comment Criteo utilise et protège leurs données. Lorsqu'un internaute décide de se désinscrire, nous arrêtons immédiatement le suivi et le reciblage. Nous supprimons ensuite tous les identifiants de leurs navigateurs, ce qui nous empêche de les cibler ultérieurement. D'après la réglementation de l'UE sur la protection des données, aucune donnée concernant un client ne peut être conservée plus de 13 mois.

Leader de notre industrie : investir dans la normalisation et les certifications

Criteo a déjà mis en place un grand nombre de certifications, qui sont révisées annuellement par des organismes officiels de certifications, dont :

- Les standards de la Network Advertising Initiative (NAI)
- L'IAB Europe
- Les principes d'autorégulation de la Digital Advertising Alliance concernant le ciblage comportemental en ligne
- Les principes d'autoréglementation de la Digital Advertising Alliance de l'Union Européenne
- Les principes d'autorégulation de la Digital Advertising Alliance du Canada
- La certification TrustArc Trusted Data Collection

Quelles sont vos responsabilités ?

Le RGPD exige des sociétés situées dans les pays de l'UE ou récupérant des données depuis ces pays de respecter les nouveaux règlements de protection et de sécurité des données. Ceci s'applique aussi aux multinationales basées en dehors de l'UE, si ces dernières visent un public au sein de l'UE. Le RGPD peut profiter à votre entreprise en consolidant les différentes lois de confidentialité des données existantes dans les 28 Etats membres. Criteo accompagne ses clients et partenaires dans les étapes leur permettant de se conformer aux normes imposées par le RGPD. Voici, entre autres, quelques meilleures pratiques pour commencer votre parcours de conformité :

Désignez un délégué à la protection des données (DPD)

Le RGPD exige la désignation d'un délégué à la protection des données (DPD) chaque fois que :

- le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des

personnes concernées; ou les activités essentielles du contrôleur ou du responsable du traitement sont le traitement à grande échelle de données sensibles (données révélant des origines raciales ou ethniques, des opinions politiques, des croyances religieuses ou philosophiques, un état de santé ou une orientation sexuelle, etc.) ou des données personnelles associées aux condamnations ou infractions pénales.

Le délégué à la protection des données doit surveiller et gérer à la fois les données et les opérations nécessaires selon les règlements. De plus, il peut avoir à prouver l'absence de conflit d'intérêt en matière de protection des données pour votre entreprise.

Assurez-vous que votre DPD est prêt à collaborer

Vos salariés sont les mieux placés pour identifier les lacunes des politiques de protection des données actuelles de votre entreprise. Assurez-vous que le DPD, les équipes juridiques, de conformité et informatiques ont une compréhension claire et complète des pratiques de traitement des données de votre entreprise. Ils doivent collaborer pour contribuer à la création d'une procédure conforme de collecte collaborative des données par votre entreprise.

Assurez la transparence et le contrôle

Les informations et la formule de consentement proposées à vos clients doivent être aussi claires et transparentes que possible. Votre site web doit expliciter clairement les options d'adhésion ou de refus choisies, et les types exacts de données que les utilisateurs vous fournissent. Ce principe est un facteur essentiel de conformité au RGPD.

Donnez la priorité à la gouvernance des données

Il est important de mettre en place une procédure d'analyse d'impact relative à la protection des données et consultation préalable (en anglais Privacy Impact Assessment ou « PIA ») pour tous les traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes p. De plus, votre entreprise doit être en mesure d'expliquer comment les données personnelles sont collectées, utilisées, ou même modifiées, et disposer de procédures permettant aux citoyens de l'UE d'accéder, rectifier ou d'obtenir l'effacement de ses données en toute simplicité. Le RGPD affirme qu'il est obligatoire d'assurer que votre entreprise conserve un registre des activités de traitement et assure la visibilité sur la conformité de vos pratiques.

Surveillez l'accès aux données des salariés et des sous-traitants

Vous devez définir des politiques strictes d'autorisation des salariés limitant l'accès aux données et assurant la confidentialité. Ces politiques doivent être constamment mises à jour en fonction des besoins de l'entreprise et permettre l'identification d'éventuelles failles, en particulier pour les transferts de données. Selon le Chapitre V du RGPD, les destinations de transfert en dehors de l'UE doivent aussi répondre aux mêmes conditions de protection et de gouvernance que celles situées dans l'UE.

Les exigences du RGPD sont strictes : bien se préparer ne se limite pas à cocher des cases sur une liste. Le RGPD tel que nous le voyons est une véritable avancée, pour les entreprises comme pour les consommateurs, car il offre cohérence et certitude sur la confidentialité et la protection des données.

En quoi le RGPD affecte-il les solutions Criteo ?

La fonction Criteo Shopper Graph est au cœur de notre technologie : elle permet de rassembler les données de comportement d'achat collectées à travers l'écosystème Commerce marketing de Criteo, et d'alimenter nos solutions de commerce marketing.

Le Criteo Shopper Graph regroupe trois types de données essentielles:

- Identifiants techniques pseudonymisés
- Intérêts des consommateurs pour les produits et services
- Mesure de la performance de nos services

Nous veillons sans cesse à ce que ces données soient utilisées uniquement dans la mesure strictement nécessaire pour fournir nos services, et donner aux consommateurs les informations pertinentes sur les produits qui les intéressent, au bon endroit, au bon moment et avec les bons messages. Exemple :

- Criteo utilise des algorithmes de hachage robustes afin qu'aucune information d'identification directe ne soit stockée dans nos systèmes.
- Nous ne stockons aucune donnée plus longtemps que nécessaire et respectons les recommandations des autorités de protection des données (DPA) de l'UE en matière de cookies et de marketing digital.
- Nous utilisations des mécanismes faciles d'utilisation : tous les produits Criteo disposent des mêmes processus simples de désinscription, accessibles sur toutes nos annonces et via notre politique de confidentialité. Criteo adhère aux normes de la NAI, aux principes de la DAA et bénéficie de la plateforme de désabonnement d'IAB Europe permettant aux consommateurs de s'opposer aux annonces ciblées.
- Les consommateurs peuvent facilement se désinscrire des services Criteo en cliquant sur le lien Ad Choices de l'annonce, mais aussi comprendre pourquoi ces annonces s'affichent. Une fois la désinscription effectuée, les informations collectées sont effacées ou rendues irrécupérables, y compris les données utilisateurs saisies lors de l'implémentation de campagnes Criteo.

Conclusion

Les entreprises dans le secteur du marketing digital mettant régulièrement à jour leurs pratiques afin de se conformer au RGPD doivent prendre en compte que les citoyens européens sont au fait du ciblage publicitaire, qu'ils comprennent globalement les identifiants sur lesquels il repose, et qu'ils souhaitent visualiser des publicités pertinentes. Criteo s'est associé à IPSOS[3] pour mener une enquête sur le terrain auprès de consommateurs européens, afin de comprendre leurs attentes et leur ressenti vis-à-vis des annonces publicitaires ciblées en ligne. Trois mille internautes (de 16 à 65 ans) ont été interrogés, en France, au Royaume-Uni et en Espagne, échantillon garantissant la représentativité démographique (sexe, âge, région et niveau de revenus).

[3] *Étude Criteo-IPSOS, 2017*

Et les résultats sont les suivants :

- 90 % des internautes connaissent les principes du ciblage comportemental
- 68 % savent que les cookies permettent de cibler une publicité
- 75 % s'attendent à voir des publicités correspondant à leurs centres d'intérêt
- 73 % préféreraient voir des publicités pertinentes plutôt que de devoir payer des frais supplémentaires pour ne plus en avoir

Criteo met un point d'honneur à protéger la confidentialité des consommateurs et à adopter une approche claire et transparente de ses pratiques. Pour renforcer la confiance et la loyauté des consommateurs, il est impératif d'informer ces derniers de l'utilisation faite de leurs données, et de leur laisser le contrôle de leurs données de navigation.

Chez Criteo, nous sommes familiers avec les principes-clés et implications du RGPD, et sommes heureux d'aider nos clients et partenaires à mieux comprendre nos produits et services. Travailler ensemble pour mieux comprendre cette nouvelle réglementation, c'est assurer la prospérité de nos entreprises.