Réponses aux questions du questionnaire

1. Qu'est-ce que le RGPD ?

Un règlement de l'UE juridiquement contraignant qui régit la manière dont les organisations et les entreprises utilisent et préservent l'intégrité des données à caractère personnel

Depuis le 25 mai 2018, le Règlement général sur la protection des données (RGPD) est un règlement du droit communautaire sur la protection des données et la confidentialité pour tous les individus dans l'Union européenne (UE) et l'Espace économique européen (EEE). Il traite également de l'exportation de données à caractère personnel en dehors de l'UE et de l'EEE. Dans un monde de plus en plus axé sur les données, le RGPD vise principalement à donner aux individus le contrôle de leurs données à caractère personnel et à simplifier l'environnement réglementaire du commerce international en unifiant la réglementation au sein de l'UE.

2. Pourquoi la réglementation est-elle vraiment importante ?

Elle renforce les droits des utilisateurs et clarifie les responsabilités des responsables du traitement des données et des sous-traitants

Le RGPD renforce les droits de toutes les personnes participant au traitement des données et définit les rôles et les responsabilités des responsables du traitement des données et des sous-traitants dans une législation européenne standardisée et claire. Il est également important de le respecter car des amendes importantes sont imposées en cas d'infraction.

3. Qu'exige le RGPD ?

La mise en place de mesures techniques et organisationnelles pour garantir la sécurité des données, notamment un contrat entre le responsable du traitement des données et le sous-traitant, ainsi que la notification à l'autorité de contrôle des violations des données à caractère personnel avec contrôle de la localisation et du transfert des données

Le RGPD établit la licéité des opérations de traitement, tient un registre des activités de traitement et garantit les droits des personnes concernées. Il met en œuvre des mesures techniques et organisationnelles pour assurer la sécurité des données et leur conformité avec les principes de la protection de la confidentialité, en établissant un contrat pour la relation entre le responsable du traitement des données et le sous-traitant au moyen d'un accord de traitement des données. Il prévoit également la notification à l'autorité de contrôle des violations de données à caractère personnel avec contrôle de la localisation et du transfert des données, et la désignation d'un délégué à la protection des données si nécessaire.

4. Comment le RGPD définit-il les « données à caractère personnel » ?

Toute information concernant une personne physique identifiée ou identifiable

Par « données à caractère personnel », on entend toute information concernant une personne physique identifiée ou identifiable (ci-après dénommée « la personne concernée »). Une « personne physique identifiable » est définie comme 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 un ou plusieurs éléments spécifiques de son identité physique, physiologique, génétique, psychologique, économique, culturelle ou sociale.

5. Qu'est-ce que le RGPD considère comme un consentement légal ?

Une action claire par laquelle la personne concernée exprime librement et de manière spécifique son consentement au traitement des données à caractère personnel

Selon le RGPD, le consentement doit être donné par le biais d'un acte positif clair par lequel la personne concernée exprime librement, de manière spécifique, en connaissance de cause et sans équivoque son consentement au traitement des données à caractère personnel, par exemple au moyen d'une déclaration écrite, y compris par des moyens électroniques, ou une déclaration orale. Cela peut se faire en cochant une case lors de la consultation d'un site web, en sélectionnant certains paramètres techniques pour les services informatiques ou au moyen de toute autre déclaration ou tout autre comportement indiquant clairement que la personne concernée accepte le traitement proposé de ses données à caractère personnel. Il ne peut donc y avoir consentement en cas de silence, de cases cochées par défaut ou d'inactivité. Le consentement donné doit s'appliquer à toutes les activités de traitement ayant la ou les mêmes finalités. Si le traitement a plusieurs finalités, un consentement doit être donné pour chacune d'entre elle. Si le consentement de la personne concernée est donné à la suite d'une demande par voie électronique, la demande doit être claire et concise, et ne doit pas nécessairement perturber l'utilisation du service pour lequel il est donné.

6. Quelle est l'amende maximale en cas de non-respect du RGPD ?

20 millions d'euros (€) ou jusqu'à 4 % du chiffre d'affaires mondial annuel

Les contrevenants au RGPD peuvent se voir infliger une amende allant jusqu'à 20 millions d'euros (€) ou jusqu'à 4 % du chiffre d'affaires mondial annuel de l'exercice précédent dans le cas d'une entreprise, le montant le plus élevé étant retenu. Les amendes sont basées sur plusieurs facteurs, notamment : la nature de l'infraction, l'intention, les mesures prises pour atténuer les dommages causés aux personnes concernées, les mesures préventives en place, la coopération avec les autorités et le type de données.

Quelle est l'amende la plus élevée à ce jour pour non-respect du RGPD ?

L'amende de la CNIL France infligée à Google.
Le 21 janvier 2019, le comité restreint de la CNIL a infligé une pénalité financière de 50 millions d'euros (€) à Google, conformément au RGPD, pour manque de transparence, informations insuffisantes et manque de consentement valide concernant la personnalisation des publicités.

7. Dans le contexte du digital analytics, quelle condition le fournisseur doit-il remplir pour que la collecte de données soit conforme au RGPD ?

Il doit obtenir le consentement des utilisateurs

L'article 6 du RGPD stipule qu'il est obligatoire d'obtenir le consentement de la personne concernée, qu'elle ait « consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ». Mais le RGPD précise également d'autres obligations du responsable du traitement des données, telles que l'obligation d'informer (articles 13 et 14) et l'obligation de répondre aux droits des personnes concernées (articles 15, 16, 17, 18, 19, 20, 21).

8. Parmi les données analytics collectées, quelles catégories de données sont considérées comme étant à « caractère personnel » ?

Adresses IP, cookies, nom du site consulté et heure de consultation de la page

Dans le cadre des définitions données par l'article 4 du RGPD, nous considérons que toutes les données que nous collectons sont considérées comme des « données à caractère personnel » et nous leur accordons la même attention et le même niveau de protection.

9. Dans le cadre du digital analytics, y a-t-il des moyens d'être exempté de la nécessité de recueillir le consentement ?

Oui, sous certaines conditions

Concernant les traceurs de mesure d'audience, la CNIL exempte le recueil du consentement dans certaines conditions que le responsable du traitement des données et le sous-traitant doivent respecter. AT Internet facilite l'application de cette exemption.

10. L'une des obligations du RGPD est de tenir des registres des activités de traitement. Que doit contenir ce document ?

Les finalités du traitement, une description des catégories de personnes concernées et des catégories de données à caractère personnel

Ces points sont précisés dans l'article 30 du RGPD. En ce qui concerne la solution de digital analytics fournie par AT Internet, nous maintenons ce document à jour pour le compte de nos clients responsables du traitement selon les conditions de forme et de contenu requises par le RGPD.