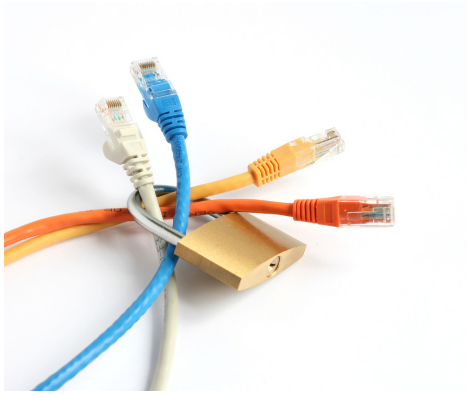
COM'COM
Département Culture & Média - Groupe Emargence

Activités culturelles : et si on passait au RGPD

N°1 | janv. 2019



I. Le RGPD, qu'est-ce que c'est ?

Fruit de quatre années de travail par la commission européenne, le règlement général sur la protection des données (RGPD) est un ensemble d'articles de lois destiné à protéger la vie numérique des citoyens de l'union européenne.

A l'heure des scandales à répétition sur les fuites de données des utilisateurs de plateformes de réseaux sociaux comme Facebook, Twitter, voire même d'entreprises du secteur financier, il devenait urgent pour la Commission Européenne de mettre en place des règles renforcées et harmonisées sur l'ensemble des pays de l'Union.

Et le moins que l'on puisse dire c'est que le RGPD ratisse large sur son application : Newsletters, réseaux sociaux, plateformes de financement participatif, fichiers d'abonnés ou de responsables de festivals, fichiers de paie des permanents et intermittents, listings informatiques de réservation, diffusions en live, billetteries, sécurisation des locaux (biométrie, caméras).

II. Suis-je concerné ?

Le RGPD s'applique à tous les acteurs économiques, les entreprises bien sûr mais également les associations culturelles. En bref, à toute entité qui traite de données de citoyens résidant sur le territoire européen.

Cette règlementation s'appliquera non seulement au Responsable de traitement des données, celui qui détermine les finalités (exemple : la gestion d'un fichier de billetterie) mais également aux éventuels sous-traitants.

III. Qu'est-ce qu'une donnée personnelle ?

D'après le RGPD, une donnée personnelle est « toute information se rapportant à une personne physique identifiée ou identifiable » que ce soit directement (nom ou prénom), ou indirectement (numéro client, téléphone, éléments biométriques, etc.).
Notons qu'il n'existe pas de restriction spécifique sur les fichiers professionnels comportant les données publiques d'une structure (adresse, labellisation, etc.). Par contre les informations de contact des équipes (nom, prénom, fonction, téléphone, email) sont concernées par le règlement.
Elles peuvent néanmoins être collectées en vue d'un traitement pour « motif légitime » c'est-à-dire que les personnes concernées pourraient être directement intéressées par vos propositions.

Illustration :
Un fichier informatique ou une base de données contenant des informations de géolocalisation, l'âge, les préférences cinématographiques, est considéré comme un traitement de données personnelles.
Pour les associations, ces données personnelles sont généralement liées à leurs membres, leurs bénévoles, donateurs, employés et partenaires y compris les contacts via leurs sites internet.
Également, les vidéos (captation de spectacles, retransmissions) sont des données personnelles encadrées par les droits d'auteurs dont le traitement devra se conformer au RGPD.

IV. Et les données sensibles ?

Avant toute chose, il convient de rappeler que selon l'article 9 de la loi informatique et libertés, le traitement de données révélant l'origine prétendue raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance

syndicale, ainsi que le traitement de données concernant la génétique, la santé ou la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.

De même, le traitement qui révèlent des données judiciaires relatives aux condamnations pénales et aux infractions sont interdits.
Il existe toutefois des exceptions qui concernent, entre autres, les motifs d'intérêt public, de santé publique, obligation en matière de droits du travail, sécurité sociale ou encore la sauvegarde des intérêts vitaux d'une personne.

Les entreprises qui traitent de données sensibles sont dans l'obligation de conduire une analyse d'impact sur la protection des données (PIA : Privacy Impact Assessment).
Cette analyse doit permettre d'identifier les points critiques sur le processus de traitement de ce type de données afin de pouvoir mieux répondre aux risques potentiels (cambriolage de l'entreprise, vols de données informatiques, etc.)

V. Qu'est-ce qu'un traitement de données ?

En quelques mots, il s'agit de toute opération appliquée à des données personnelles, que ce soit via des moyens informatisés ou non. Par exemple, la collecte d'informations pour une carte d'abonnement, la conservation des données, leur transfert, leur diffusion, etc.

L'achat d'une base de données dans le cadre d'une campagne promotionnelle est également considéré comme un traitement.
Une des notions phares du RGPD concerne la finalité du traitement ; chaque donnée collectée doit servir un but, un objectif précis. Il n'est donc pas autorisé de récupérer des informations sous prétexte qu'elles pourraient être utiles ultérieurement.

Autre notion importante, celle de la « minimisation » du volume des données traitées. Elle va de pair avec la notion de finalité dont l'objectif est de limiter au maximum le nombre d'informations transmises. Ces règles doivent permettre de réduire les risques de retrouver potentiellement « dans la nature » des données sans rapport avec les traitements.

VI. Et le papier dans tout ça ?

Notez que les fichiers au format papier doivent aussi être protégés au même titre que leurs versions numériques : seules les personnes autorisées doivent y avoir accès, données stockées dans des endroits protégés cette fois-ci physiquement (placards ou tiroirs verrouillés, locaux sous vidéo surveillance, etc.).

VII. Concrètement, qu'est-ce que tout cela signifie ?

Tout d'abord, il doit y avoir une prise de conscience : tous les acteurs de la vie économique sont désormais potentiellement impliqués dans la protection des données personnelles.
Les entreprises doivent se poser des questions importantes et être capables d'y répondre efficacement :
• Est-ce que les données sont utilisées avec le consentement éclairé et explicite des personnes ?
• Les contrats sont-ils suffisamment précis sur les informations collectées, leur nécessité et les objectifs attendus ?
• Est-ce que la procédure de collecte, de traitement, de stockage a fait l'objet d'une analyse de sécurité ?
• Que se passerait-il si les outils informatiques contenant les coordonnées bancaires des clients étaient piratés ?

VIII. Quelles sanctions en cas de non respect ?

Selon la gravité du dysfonctionnement constaté et lié au RGPD, notamment lorsqu'il s'agit d'un des manquements aux obligations du responsable de traitement (ou du sous-traitant), une amende d'un montant de 2 % du chiffre d'affaires mondial pour les entreprises ou 10 millions d'euros d'amende peut être appliqué.
Et cela peut également aller jusqu'à une amende qui correspond à 4 % du chiffre d'affaires mondial ou 20 millions d'euros sur des infractions liées aux obligations de consentement de la personne, ses droits et non-respect d'injonctions précédentes.

Outre les sanctions financières, l'impact en termes d'images est également non négligeable car la CNIL peut décider de communiquer de manière publique sur des avertissements, injonctions et pénalités infligées aux entreprises concernées.

Conclusion

Cette loi est complexe et nécessite une mise en place avec réflexion et organisation.
Dans un premier temps, les sanctions se limiteront à des avertissements mais très rapidement il s'agira d'être en conformité.
N'hésitez pas à nous en parler, nous saurons vous conseiller et vous accompagner dans cette démarche.