Comment mettre votre business créatif en conformité avec le RGPD | Règlement Général sur la Protection des Données

by admin_Crefovi - lundi, octobre 16, 2017

https://crefovi.fr/articles/comment-mettre-votre-business-creatif-en-conformite-avec-le-rgpd/

Le RGPD arrive à grands pas: qu'est-ce que c'est? Comment est-ce qu'il va impacter vous-même et votre business? Que devez-vous faire afin de vous mettre en conformité avec le RGPD?

Il n'y a pas un moment à perdre, étant donné que les enjeux sont très élevés, et puisqu'être en conformité avec le RGPD va bien évidemment procurer des avantages concurrentiels à votre business.

Le 27 avril 2016, après plus de 4 ans de discussions et négociations, le parlement et le conseil européens ont adopté le Règlement Général sur la Protection des Données (« **RGPD** »).

1. Pourquoi le RGPD?

Le RGPD abroge la Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (la "**Directive**").

La Directive, qui est entrée en vigueur il y a plus de 20 ans, n'était plus propre à l'usage, étant donné que la quantité d'informations numériques que les entreprises créent, capturent et stockent, a beaucoup augmentée.

Les données – et plus il y en a, mieux c'est – sont là pour durer. Les données d'aujourd'hui lubrifient de plus en plus notre monde numérique. Le contrôle des données est, en fin de compte, constitutif de pouvoir, et la propriété des données a un effet très sérieux sur la concurrence dans tout marché existent. En collectant plus de données, une entreprise a plus de champ pour améliorer ses produits, ce qui attire plus d'utilisateurs, générant encore plus de données, et ainsi de suite. Les actifs constitués par les données (« data assets ») sont, aujourd'hui, au moins tout aussi importants que les autres actifs intangibles tels que les marques, le droit d'auteur, les brevets et dessins et modèles, pour les sociétés[1]. Les enjeux sont beaucoup plus élevés, aujourd'hui, en ce qui concerne la propriété, le contrôle et la gestion des données, et le RGPD est focalisé sur ce flot de données du 21ème siècle, alors que nous nous impliquons de plus en plus avec la technologie.

De plus, de nombreux cas judiciaires, lancés dans plusieurs états-membres de l'Union Européenne ("**UE**"), ont mis le doigt sur les sévères faiblesses et lacunes existantes, en terme de fourniture d'une protection des données personnelles – relatives aux citoyens de l'UE – satisfaisante, forte et homogène, et contrôlées par des sociétés et businesses opérant dans l'UE. Par exemple, le jugement Costeja v Google, rendu par la Cour de justice de l'Union Européenne (« **CJUE** »), auquel il est souvent fait référence sous l'appellation « jugement sur le droit à l'oubli », a été rendu le 26 novembre 2014. Ce jugement novateur a reconnu que les opérateurs de moteurs de recherche, tels que Google, gèrent des données personnelles et appartiennent à la catégorie de responsables de traitement (« data controllers ») au sens de l'Article 2 de la Directive. De ce fait, la décision de la CJUE reconnaît qu'une personne physique puisse "*requérir (auprès d'un moteur de recherches) que les informations (relatives à lui ou elle, personnellement) ne soient plus mises à la disposition du public du fait de son inclusion dans (…) une liste de résultats*". Par le biais de cette décision, la CJUE a forcé les moteurs de recherche tels que Google à retirer, quand demandé, les liens URL qui sont "*inadéquats, hors de propos ou ne sont plus pertinents, ou excessifs en relation avec le but pour lequel ils ont été traités et au vue du temps qui s'est écoulé*". Cet arrêt a marqué un grand pas en avant pour la protection des données personnelles dans l'UE.

En outre, les piratages informatiques dans, et les cyber-attacks de, milliers d'entreprises multinationales (Sony Pictures, Yahoo, Linkedin, Equifax, etc.) ainsi que de sociétés nationales de l'UE (Talktalk, etc.) font la une, constamment et de manière très régulière, affectant de manière dramatique le bien-être financier et moral de millions de consommateurs dont les données personnelles ont été volées à cause de ces piratages informatiques. Ces attaques et piratages soulèvent de très graves inquiétudes en ce qui

concerne l'aptitude des businesses gérant les données personnelles des consommateurs de l'UE à être à la hauteur, en termes de lutter de manière proactive contre la cybercriminalité et de protéger les données personnelles.

Enfin, le RGPD, qui sera immédiatement applicable dans les 28 états-membres de l'UE sans aucune transposition à partir du 25 mai 2018 (à la différence de la Directive qui avait dû être transposée dans chaque état-membre de l'UE par des réglementations nationales), standardise toutes les lois nationales applicables dans ses états-membres et par conséquent apporte une uniformité parfaite entre elles. Le RGPD met tous les états-membres sur un pied d'égalité.

2. Quand le RGPD entrera-t-il en vigueur?

Le RGPD, adopté en avril 2016, entre en vigueur le 25 mai 2018, fournissant idéalement une période de préparation de 2 ans aux businesses et entités du secteur public pour qu'ils s'adaptent aux changements.

Alors que de nombreux gérants d'entreprises de l'UE adoptent le point de vue que les changements apportés par le RGPD à leurs businesses, seront d'importance soit mineure soit nulle, ou seront du même ordre d'importance que d'autres problématiques de compliance, il n'y a pas une minute à perdre pour se préparer à la mise en conformité avec le nouveau jeu de règles longues et complexes énoncées dans le RGPD.

3. Quels sont les enjeux? Quelles organisations sont impactées par le RGPD?

Les enjeux sont très importants. toutes les sociétés, organisations ou entités qui opèrent dans l'UE ou qui ont leurs sièges hors de l'UE mais qui collectent, détiennent ou traitent des données personnelles de citoyens de l'UE doivent se mettre en conformité avec le RGPD avant le 25 mai 2018. Potentiellement, le RGPD pourrait s'appliquer à tout site internet et à toute application sur une base globale.

Comme la plupart, si ce n'est toutes, les multinationales ont des clients, employés et/ou partenaires commerciaux dans l'UE, elles doivent se mettre en conformité avec le RGPD. Même les start-ups et PME doivent se mettre en conformité avec le RGDP, si leur business model implique qu'elles vont collecter, détenir ou traiter des données personnelles de personnes physiques de l'UE (c'est à dire les consommateurs, prospects, salariés, contractants et contractuels, fournisseurs, etc).

Les enjeux sont très élevés pour la plupart des businesses et, pour de nombreuses sociétés, cela devient une problématique et une conversation qui se déroule au niveau du top management et du conseil d'administration.

Pour assurer la mise en conformité avec le nouveau système juridique sur la protection des données, et le respect des nouvelles dispositions, le RGPD a introduit un système de poursuites avec des sanctions financières très lourdes qui seront imposées aux businesses qui ne sont pas en conformité. Si une organisation ne traite par les données personnelles des personnes physiques de l'UE de manière

appropriée, elle peut être sanctionnée à payer une amende pouvant aller à, soit 4% de son chiffre d'affaires annuel global, soit 20 millions d'euros – quel que soit le montant le plus élevé[2].

Ces amendes futures sont bien plus élevées que la somme de GBP500.000 d'amende plafonnée que l'Autorité de Protection des Données Personnelles (« **APDP**«) du Royaume Uni, l'Information Commissioner Office ("**ICO**"), ou la somme de 300.000 euros d'amende plafonnée que l'APDP française, la Commission Nationale Informatique et Libertés ("**CNIL**"), peuvent infliger à des personnes morales actuellement.

4. Que couvrent les dispositions du RGPD?

Le RGPD est constitué de 99 articles énonçant les droits des personnes physiques, et les obligations placées sur les organisations et personnes morales, dans le champ du RGPD.

Comparé à la Directive, voici les concepts clé nouveaux apportés par le RGPD.

4.1. Privacy by design

Le principe de « privacy by design » signifie que les businesses doivent prendre une approche proactive et préventive en relation avec la protection de la vie privée et des données personnelles. Par exemple, un business qui limite la quantité de données personnelles collectées, ou qui anonymise ces données, est conforme au principe de "privacy by design".

Cette obligation de "privacy by design" implique que les businesses doivent intégrer – par tous moyens techniques appropriés – la sécurité des données personnelles dès le lancement de leurs applications ou procédures commerciales.

4.2. Responsabilité (« Accountability »)

La responsabilité (« accountability ») signifie que le responsable du traitement (« data controller »), ainsi que le sous-traitant (« data processor »), doit prendre des mesures juridiques, organisationnelles et techniques appropriées leur permettant de se mettre en conformité avec le RGPD. En outre, les responsables de traitement et les sous-traitants doivent pouvoir démontrer l'exécution de ces mesures, en toute transparence et à tout moment dans le temps, tant auprès de leurs APDP respectifs, qu'auprès des personnes physiques dont les données personnelles ont été traitées par eux.

Ces mesures doivent être proportionnées au risque, c'est à dire au préjudice qui serait causé aux personnes physiques de l'UE, en cas d'utilisation inappropriée de leurs données personnelles.

Afin de savoir si un business est en conformité, il est par conséquent nécessaire d'exécuter un audit des processus relatifs aux données personnelles d'une telle société. Notre cabinet d'avocats Crefovi exécute souvent des audits certifiés par la CNIL ou le ICO.

4.3. Etude d'impact (« Privacy impact Assessment »)

La société en charge de traiter et gérer les données personnelles, ainsi que ses sous-traitants, doit faire une analyse, une étude d'impact aussi appelée « Privacy Impact Assessment » ("**PIA**") relative à la protection des données personnelles.

Les businesses doivent exécuter un PIA, une étude d'impact, sur leurs actifs constitués par des données personnelles (« data assets »), afin de suivre et de cartographier les risques inhérents à chaque processus et traitement de données mis en place, en fonction de leur plausibilité et de leur sérieux. A côté de ces risques, le PIA énonce la liste des mesures organisationnelles, technologiques, physiques et juridiques mises en oeuvre pour adresser et minimiser ces risques. Le PIA a pour but de vérifier l'adéquation de ces mesures et, si ces mesures échouent ce test, à déterminer des mesures proportionnées pour adresser ces risques découverts et pour s'assurer que le business devienne conforme au RGPD.

Crefovi accompagne les sociétés dans l'exécution de PIAs et en vérifiant l'efficacité des mesures de protection et de sécurité, grâce à l'exécution de tests d'intrusion.

4.4. Correspondant informatique et liberté (« Data Protection Officer »)

Le RGPD requiert qu'un officier de la protection des données (« Data Protection Officer », "**DPO**") soit nommé, afin d'assurer la conformité du traitement des données personnelles par les administrations publiques et les entreprises dont les traitements de données personnelles présentent un fort risk de violation de la protection de la vie privée. Le DPO est le porte-parole de l'organisation en relation avec les données personnelles: il ou elle est le point de contact à qui s'adresser, pour le APDP, en relation avec la mise en conformité du traitement des données personnelles, mais aussi pour les personnes physiques dont les données ont été collectées, afin qu'elles puissent exercer leurs droits.

En plus d'avoir les prérogatives de correspondant informatique et liberté ("**CIL**") en France, ou « chief privacy officer » au Royaume Uni, le DPO doit informer ses interlocuteurs de tout piratage informatique qui pourrait intervenir dans l'organisation, et analyser leur impact.

4.5. Profiling

Profiling est un processus automatisé des données personnelles permettant la construction d'informations complexes concernant une personne particulière, telles que ses préférences, sa productivité au travail ou ses allées et venues.

Ce type de traitement des données personnelles peut générer une prise de décision automatisée, qui peut avoir des conséquences juridiques, sans aucune intervention humaine. De ce fait, profiling constitue un risque aux libertés individuelles. C'est pour cela que les entreprises faisant du profiling doivent limiter ses risques et garantir les droits des personnes physiques qui font l'objet de ce profiling, en particulier en leur permettant de requérir une intervention humaine et/ou de contester la décision automatisée.

4.6. Droit à l'oubli

Comme expliqué ci-dessus, le droit à l'oubli permet à une personne physique d'éviter que des informations concernant son passé interfèrent avec sa vie actuelle. Dans le monde numérique, ce droit

comprend le droit à l'effacement ainsi que le droit au déréférencement. D'un côté, la personne peut avoir du contenu potentiellement nocif effacé du réseau numérique, et, de l'autre côté, la personne peut dissocier un mot clé (tel que son prénom et son nom de famille) de certaines pages web sur un moteur de recherche.

Crefovi peut conseiller un business faisant face à une demande d'exécution du droit à l'oubli.

4.7. Autres droits des personnes physiques

Le RGPD complémente le droit à l'oubli en remettant les personnes physiques de l'UE fermement en contrôle de leurs données personnelles, renforçant de manière notoire l'obligation de consentement au traitement des données personnelles, ainsi que les droits des citoyens (droit à l'accès des données, droit de rectifier les données, droit de limiter le traitement des données, droit à la portabilité des données et droit de s'opposer au traitement des données personnelles), et les obligations d'information par les businesses à propos des droits des citoyens.

5. Quel est le bon côté du RGPD?

5.1. Une opportunité de gérer ces données personnelles constituant des actifs précieux

La mise en conformité avec le RGPD devrait être vu par les businesses comme une opportunité, autant qu'une obligation: alors que les données personnelles sont de plus en plus importantes dans une organisation aujourd'hui, ceci est une excellente opportunité d'évaluer quelles données personnelles votre société détient, et comme vous pouvez en tirer le plus gros avantage.

Le principe clé du RGPD est qu'il vous donnera la capacité de trouver les données personnelles dans votre organisation qui sont très sensibles et à haute valeur, et de vous assurer que ces données personnelles sont protégées de manière adéquate des risques et des piratages informatiques.

5.2. Moins de formalités et une APDP à guichet unique

En outre, le RGPD retire l'obligation de déclaration préalable auprès du APDP compétent, avant tout traitement de données personnelles, et remplace ces formalités avec la création obligatoire et la gestion d'un registre de traitement des données personnelles.

De plus, le RGPD instaure une APDP à guichet unique: en cas d'absence d'une législation nationale spécifique, une APDP localisée dans un état-membre de l'UE dans lequel l'organisation a son principal ou unique établissement sera en charge de contrôler la conformité avec le RGPD.

Les businesses détermineront leur APDP respective en se basant sur le lieu d'établissement de leurs fonctions de management, concernant la supervision du traitement des données personnelles, ce qui permettra d'identifier l'établissement principal, y compris quand une société unique gère les opérations d'un groupe entier.

Cette APDP à guichet unique permettra aux sociétés de gagner du temps et de l'argent de manière substantielle, en simplifiant leurs processus.

5.3. Règlement unifié, transferts de données facilités

Afin de favoriser le marché européen des données personnelles et l'économie numérique, et ainsi de créer un environnement économique favorable, le RGPD renforce la protection des données personnelles et des libertés fondamentales.

Cette réglementation unifiée permettra aux businesses de réduire de manière substantielle les coûts du traitement des données personnelles qui sont à ce jour engagés dans les 28 états-membres de l'UE: les organisations n'auront plus à se mettre en conformité avec des réglementations nationales multiples pour la collecte, la récolte, le transfert et le stockage des données personnelles qu'elles utilisent.

En outre, étant donné que les données personnelles seront conformes avec la législation applicable dans tous les états de l'UE, il deviendra possible d'échanger les données et elles auront la même valeur dans différents pays, alors que pour l'instant les données personnelles ont différents prix en fonction de la législation avec laquelle elles sont en conformité, ainsi que des coûts différents pour les sociétés qui les collectent.

5.4. Un champ géographique étendu par la concurrence loyale

Le champ du RGPD s'étend à des sociétés qui ont leurs siège social hors de l'UE, mais qui ont l'intention de marketer des produits et services dans le marché de l'UE, tant qu'elles ont en place des processus et traitements des données personnelles relatives à des personnes physiques de l'UE. Suivre ces résidents sur internet, afin de créer des profils, est aussi couvert par le champ du RGPD.

Par conséquent, les sociétés européennes, assujetties à des règles plus strictes, et potentiellement plus chères, ne seront pas pénalisées par la concurrence internationale sur le marché unique de l'UE. En outre, elles peuvent acheter aux entreprises non-UE certaines données personnelles qui sont conformes aux dispositions du RGPD, créant ainsi un marché des données plus large.

5.5. Ouvrir les services numériques à la concurrence

Le droit à la portabilité des données personnelles permettra aux personnes physiques de l'UE, qui font l'objet de traitement et gestion de leurs données personnelles, d'obtenir ces données personnelles sur un format exploitable ou de transférer ces données personnelles à un autre responsable de traitement (« data controller ») si cela est techniquement possible.

De cette façon, le client pourra changer de fournisseur de services numériques (email, photographies, etc.) sans avoir à manuellement récupérer toutes les données, durant un processus tant fastidieux que chronophage. En enlevant de telles barrières techniques, le RGPD rend le marché plus fluide, et offre aux utilisateurs une mobilité numérique supérieure. Les fournisseurs de services numériques vont par conséquent évoluer dans un marché plus concurrentiel, les incitant à fournir des services à meilleur marché et de plus haute qualité, étant donné que leurs clients ne seront plus les otages de leurs fournisseur

initial.

5.6. Labels et certifications

Le comité européen sur la protection des données personnelles, ainsi que les institutions de l'UE, proposeront certaines certifications et labels afin de certifier la conformité avec le RGPD des traitements de données effectués par les entreprises.

Des reconnaissances monétaires et de vrais actifs pour l'image de marque d'une entreprise, les labels et certifications deviendront aussi un outil commercial important afin de gagner la confiance des prospects et pour obtenir leur loyauté.

6. Quelles sont les étapes concrètes à suivre, aujourd'hui, pour être en conformité avec le RGPD?

Il n'y a pas un moment à perdre pour mettre en oeuvre les étapes suivantes, ci-dessous

- Décider qui à la responsabilité de mettre en oeuvre les dispositions du RGPD dans votre organisation; assigner cette responsabilité au département ou à l'équipe le plus ou la plus approprié(e) (Service juridique? Compliance? Technologie IT?);
- Correspondre avec l'APDP à guichet unique, puisque plusieurs d'entre elles ont préparé des informations explicatives et des guides sur la mise en conformité avec le RGPD, telles que le ICO au Royaume Uni, la CNIL en France et le Data Protection Commissioner en Irlande (ce dernier étant l'APDP de nombreux géants numériques, tels que Google, Facebook et Twitter);
- Préparer une cartographie des traitements de données dans votre organisation, et identifier les lacunes dans la conformité avec le RGPD en relation avec ces différents processus – nous, avocats du cabinet d'avocats Crefovi, avons rédigé des documents détaillés sur comment faire cette cartographie des traitements et du processing de données et pour vous épauler pour identifier les lacunes dans la conformité avec le RGPD;
- Valoriser les différents processus et traitements de données personnelles et évaluer lesquels sont à haut risque et faire une liste de vos données personnelles constituant des actifs ((« data assets ») à haut risque;
- Exécuter un étude d'impact ou PIA sur ces data assets à haut risque (telles que les données des ressources humaines, les données personnelles des clients) – Crefovi épaulent les sociétés dans la mise en place des PIAs et pour vérifier l'efficacité des mesures de sécurité et de protection, grâce à l'exécution de tests d'intrusion;
- Mise en oeuvre de mesures juridiques, techniques, organisationnelles et physiques pour réduire les risques sur ses data assets se mettre en conformité avec le RGPD;

- S'assurer que vos contractants et sous-contractants ont mis en place des mesures de sécurité conformes, en leur envoyant une liste des points à vérifier;

- Faire des formations de connaissance de la protection de la vie privée pour vos salariés étant donné qu'ils doivent comprendre que les données personnelles sont constituées par n'importe quoi qui peut être directement lié à une personne physique et qu'il y aura des conséquences s'ils violent les dispositions du RGPD et volent des données personnelles;

- Développer une politique « Apporter Son Propre Appareil » ("**ASPA**") et la mettre en oeuvre dans votre organisation et parmis vos salariés, étant donné que vous êtes responsable pour toutes les informations d'utilisation des données personnelles qui sont stockées dans le cloud et accessibles depuis tant des appareils d'entreprise (tablettes, smartphones, ordinateurs portables) que des appareils personnels. Aussi, quand les salariés partent ou sont licenciés, assurez-vous que vous avez inclus ASPA dans votre processus de fin de contrat de travail, afin que le personnel partant perde accès aux données personnelles de la société immédiatement sur leurs appareils;

- Vérifier et/ou amender les notifications d'information ou les politiques de confidentialité afin qu'elles tiennent en compte les nouvelles informations requises par le RGPD;

- Mettre en place des mécanismes automatisés afin d'obtenir le consentement explicite des personnes physiques résidentes dans l'UE, particulièrement si votre business est impliqué dans la collection de données comportementales, la publicité comportementale ou tout autre forme de profiling;

- Mettre en place un plan de management solide au cas où des piratages informatiques de données personnelles ont lieu, ce qui vous permettra d'être en conformité avec les conditions obligatoires de notification de votre APDP en 72 heures – notre expérience approfondie de plans d'alerte, de plans de risk management, de plans analytiques et de plans de notification, en France et au Royaume Uni, nous place, chez Crefovi, dans une position adéquate pour épauler nos clients dans leur mise en conformité avec les exigences contraignantes énoncées dans le RGPD.

[1] "*The world's most valuable resource is no longer oil, but data*", The economist, 6 Mai 2017.

[2] "*Preparing for the general data protection regulation: a roadmap to the key changes introduced by the new European data protection regime*", Alexandra Varla, 2017.

Annabelle Gauberti est l'associée fondatrice de Crefovi, notre cabinet d'avocats basé à Londres et Paris spécialisé dans le conseil aux industries créatives en général, en particulier sur leurs besoins en matière de protection des données personnelles et contre les piratages informatiques. Elle est un avocat au barreau de Paris et un solicitor of England & Wales.

Annabelle est aussi présidente de l'International association of lawyers for the creative industries (ialci).

Votre nom (obligatoire)

Votre email (obligatoire)

Sujet

Votre message