Vivement le RGPD !

L'opportunité de repenser sa stratégie marketing client.

Les 10 étapes à ne pas manquer vers la conformité RGPD.

Splio

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE

Sommaire

1. Avant-propos.

Vivement le RGPD! Vous vous demandez sûrement pourquoi ?

Splio et Taxmen sont deux sociétés européennes con-vain-cues de l'opportunité que représente cette nouvelle réglementation pour le commerce en Europe, et fières de l'exemple qu'offre l'EU au reste du monde.

Splio développe une plateforme marketing omnicanale en mode SaaS qui, basée sur la connaissance client, permet aux marketeurs d'aligner les stratégies de communication on et offline, d'offrir des expériences clients connectées et de générer ainsi du chiffre d'affaires.

Aux côtés de l'équipe Taxmen, agence experte en services juridiques et fiscaux en Europe, spécialisée en e-commerce, nous avons décidé de créer ce guide pour accompagner les marketeurs et les DPO, ensemble, vers la conformité RGPD.. Ce guide veillera également par ailleurs à faire prendre conscience de l'importance des données pour développer une marque, une relation client aux bases solides et les ventes.

Le RGPD est une réglementation très positive pour le commerce on et offline en Europe. Les modèles traditionnels du commerce changent et c'est également le cas des consommateurs du monde entier.

La data est devenu un moteur de croissance pour les marques, et la protection des données un thème crucial dans la relation client. Les marques doivent passer d'un **marketing B2C à un marketing C2B**, soit à une dynamique très customer-centric, insufflée depuis quelques années par les Millennials, et où la data et la fidélité client jouent un rôle clé. Ces consommateurs d'un nouveau genre sont l'avenir de la consommation et il est impératif de prendre en compte ces nouvelles considérations pour développer de nouvelles stratégies omnicanales.

Les 5 chapitres qui suivent mettront en perspective les 10 étapes clés vers la conformité RGPD, indiquant également la nécessité des équipes à travailler étroitement ensemble, de manière transversale, en vue d'implémenter la stratégie data adéquate.

2. État des lieux : êtes-vous conforme au RGPD?

25 mai 2018 : pour la première fois, un ensemble unique de **protection pour les données personnelles** va s'appliquer directement dans **tous les pays européens**.

Ce jour-là, le **Règlement Général sur la Protection des Données (RGDP)** sera applicable directement pour **remplacer** les lois actuelles des 28 pays de l'Union Européenne concernant la vie privée, qui **diffèrent** encore partiellement malgré le processus d'**harmonisation** initié par la **DPD (Directive de Protection des Données** : Directive 95/46/EC).

Quelles différences avec la DPD ? Le RGPD renforce et définit mieux les **droits fondamentaux des personnes** quant au respect du traitement de leurs **données personnelles** et aux règles relatives à la **libre circulation** des données personnelles.

Il est important de rappeler la **signification** des termes les plus fréquemment utilisés dans la DPD et maintenant le RGPD :

- Responsable du traitement **(data Controller)** : le sujet qui (seul ou avec un autre sujet) détermine les **finalités** et les **moyens** du traitement des données personnelles ;

- Sous-traitant (**data processor**) : le sujet qui traite les données personnelles **pour le compte** du responsable du traitement, le cas échéant ;
- **Personnes concernées :** les individus dont les données sont traitées (ou « détenteurs des données personnelles »).
- Le terme « **données personnelles** », est défini dans la partie 3.1.

2.1 Ce qui change : l'extension du périmètre territorial

Tout d'abord, le RGPD étend le **champ d'application territorial** de la loi : doivent s'y soumettre les organisations suivantes traitant des données personnelles :

- **les organisations européennes**, que le traitement des données ait lieu au sein de l'Union ou non ;
- **les organisations non-européennes**, lorsque le traitement concerne : (a) une offre de biens / services, même gratuite, proposée à **des résidents de l'Union** ; et/ou (b) s'il s'agit de suivre des comportements qui se déroulent au sein de l'UE ;
- **les organisations non-européennes**, mais situées dans un lieu où la loi d'un Etat de l'UE s'applique en vertu du **droit international public**.

2.2 Quels sont les principaux changements apportés à la loi sur la protection des données personnelles de l'Union européenne ?

En plus de l'extension du périmètre territorial de la loi de l'UE, les principaux changements introduits par le RGPD incluent :

- **Droits d'information** accrus : la **liste des informations** que les responsables du traitement doivent fournir aux personnes concernées inclut désormais notamment la **période de conservation** prévue des données (ou, si cela n'est pas possible, les

critères utilisés pour déterminer cette période), le droit à **l'effacement**, celui de **restreindre ce traitement**, et de déposer une **plainte** auprès d'une autorité de surveillance ;

- **Consentement :** les conditions pour que le consentement de l'utilisateur soit considéré comme le **fondement juridique** du traitement des données ont été **renforcées** ;
- **Droit à l'oubli et à la restriction du traitement :** après la jurisprudence de la Cour de Justice de l'Union européenne (CJUE), le RGPD a codifié le droit des personnes concernées de voir leurs données personnelles effacées ou leur traitement restreint, sous certaines conditions spécifiques ;
- **Notification de violation :** la notification d'atteinte à la vie privée devient obligatoire auprès de l'autorité de surveillance dès lors que la violation risque de « générer un risque pour les droits et la sécurité des individus » ;
- **DPD et DPIA :** sous certaines conditions spécifiques, le règlement a introduit l'obligation de désigner un Délégué à la Protection des Données et/ou de réaliser une Analyse d'Impact sur la Protection des Données ;
- **Représentants des entreprises non-européennes :** les entreprises non-européennes qui traitent les données personnelles tombant sous le coup de la loi sur la confidentialité de l'Union européenne sont désormais tenus de désigner par écrit un représentant dans l'Union (sauf à certaines exceptions).

Certains changements réglementaires concernent plus particulièrement les entreprises numériques par rapport aux acteurs de l'économie traditionnelle (voir partie 2).

2.3 Pourquoi vous devriez vous préparer rapidement : les obligations et les sanctions

Il est extrêmement important pour les entreprises de se conformer au RGPD dès son entrée en vigueur, sous peine de devoir, plus tard, indemniser les individus ayant souffert de préjudices matériels ou immatériels faisant suite à une violation du RGPD !

De plus, les autorités de surveillance nationales seront habilitées à appliquer des amendes administratives aux organisations non conformes (dans une limite de 20 millions d'euros ou - dans le cas d'une entreprise - jusqu'à 4% du chiffre d'affaires annuel mondial de l'exercice précédent).

3. Commerce physique vs. e-commerce.

Alors que la grande majorité des dispositions du RGPD s'adresse aussi bien aux entreprises traditionnelles qu'aux entreprises du numérique, certaines des nouvelles règles reflètent clairement les changements induits par la technologie dans l'économie mondiale au cours de la dernière décennie : elles auront donc un impact particulier sur le e-commerce.

3.1 Le RGPD et l'économie numérique

Certaines parties du RGPD semblent cibler spécifiquement les secteurs du numérique :

- **Portabilité des données**

  Sous **certaines conditions**, lorsque les données personnelles ont été générées par des moyens automatiques, les personnes concernées ont le droit de demander au responsable du traitement de les récupérer ***« dans un format ouvert, couramment utilisé et lisible par machine ».***

  En substance, la portabilité des données est le **droit** des utilisateurs ayant fourni des données personnelles à un responsable du traitement à récupérer une **partie** de ces données et/ou de les faire transmettre à un autre responsable du traitement, sans aucune entrave.

- **Données personnelles des enfants**

  L'âge minimum pour donner un consentement légal au traitement des données personnelles en relation avec une **offre de services en ligne** a été fixé à seize (16) ans. **En-deçà** de cet âge, le traitement des données personnelles ne sera licite **que si** le **parent** ou le **tuteur** y a consenti.

  Le RGPD **permet** aux États membres d'abaisser ce seuil d'âge, mais uniquement jusqu'à un minimum de **13 ans**.

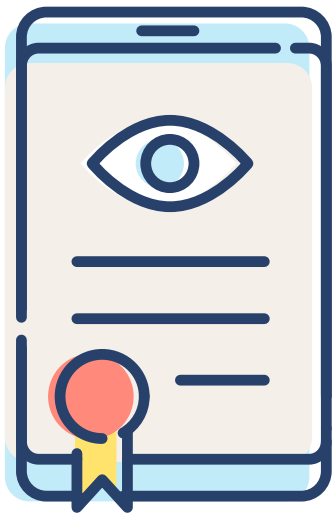
- **Respect de la vie privée « dès la conception » (qu'on appelle « Privacy by Design»**

  Le RGPD codifie le principe selon lequel les produits et services doivent être conçus en tenant compte le plus tôt possible des règles de confidentialité : par exemple en minimisant le traitement des données et en les pseudonymisant.

- **Profilage et prise de décision automatisée**

  Le RGPD inclut des règles pour protéger les individus lorsqu'une entreprise effectue des prises de décisions automatisées ayant un effet juridique (ou d'importance similaire) sur ces personnes. Les entreprises ne peuvent effectuer ce type de prise de décision que lorsque celle-ci est : nécessaire pour la conclusion ou l'exécution d'un contrat ; autorisée par la loi applicable ; ou basée sur le consentement explicite de l'individu.

3.2 Le projet de Règlement « e-privacy »



En janvier 2017, la Commission européenne (CE) a publié une proposition de nouveau **Règlement sur la vie privée et les communications électroniques** qui abrogerait la **Directive sur la vie privée et les communications électroniques** (Directive 2002/58/CE).

Comme son nom l'indique, cette proposition concerne la protection des données à caractère personnel dans le **secteur des communications électroniques.** Il vise à détailler et compléter le RGDP autour des communications électroniques qualifiées de données personnelles. Toutes les questions concernant le traitement des données personnelles qui ne sont pas traitées par la proposition restent couvertes par le RGPD.

Stay tuned : la proposition relative au Règlement sur la vie privée et les communications électroniques devrait être approuvée par le Conseil en 2018.

4. De quelles données parle-t-on ? Les données personnelles et le consentement.

Le RGPD concerne la protection des **« données personnelles »**, c'est-à-dire toute information relative à une personne **physique** identifiée ou identifiable.

Le RGPD définit ainsi la notion de **personne identifiable** : « personne qui peut être identifiée, directement ou indirectement, notamment grâce 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, mentale, économique, culturelle ou sociale ».

Les **« considérants »** du RGPD précisent que les **identifiants en ligne** incluent également les adresses **IP**, les cookies ou les tags RFID, en particulier **lorsqu'ils sont combinés** avec des identifiants uniques et/ou d'autres informations reçues par les serveurs dans le but de créer des profils de personnes physiques et de les identifier.

Au contraire, le droit de la vie privée de l'Union Européenne ne s'applique pas aux **informations anonymes**, en particulier celles qui ne se rapportent pas à une personne identifiée ou identifiable.

Le cas des données sujettes à la **pseudonymisation** est différent : elles pourraient être attribuées à une personne physique grâce à l'utilisation d'informations complémentaires. Ce type de traitement est autorisé, voire même **encouragé** dans

certains cas, tant que ces informations complémentaires sont conservées séparément et font l'objet de mesures techniques et organisationnelles capables de garantir que les données personnelles ne peuvent être attribuées à une personne spécifique.

4.1 Les catégories spéciales de données (données sensibles)

Sauf dans le cas de **dérogations - mais toujours limitées -**, il existe des catégories spéciales de données personnelles dont le traitement est formellement interdit par la loi : « les données personnelles révélant l'origine raciale ou ethnique d'une personne, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance à un syndicat, ainsi que le traitement des données génétiques ou biométriques dans le but d'identifier une personne physique, les données concernant la santé ou la vie / l'orientation sexuelle d'une personne physique ».

Le RGPD permet de déroger à cette interdiction de traiter les catégories spéciales de données à caractère personnel dans certains cas. Par exemple, si la personne concernée a donné son consentement dans un ou plusieurs buts spécifiques et que la loi applicable ne l'empêche pas de le faire.

4.2 Consentement

Les règles sur le **consentement** sont devenues **plus strictes** dans le cadre du RGPD.

Suite à diverses décisions de la Cour de Justice de l'Union européenne, le RGPD a codifié en droit les principes concernant le consentement de la **personne concernée** au traitement de ses données personnelles :

- La **demande de consentement** à la personne concernée doit être clairement **distincte** de toute autre demande, communication ou information soumise ; elle doit être **intelligible**, facilement accessible et exprimée dans un langage clair et simple ;
- Le consentement doit être donné par un **acte positif** clair reflétant un « accord donné de façon libre, spécifique, informée et **univoque** » ;
- **Le silence, les cases pré-cochées ou l'inactivité** ne constituent **pas** un consentement ;
- Le consentement est présumé ne pas être donné librement lorsque la personne concernée est empêchée d'exprimer un consentement distinct pour chacun des différents traitements de ses données personnelles, ou lorsque le rendu d'un service **dépend** de son consentement au traitement de ses données (lorsqu'il n'est pas nécessaire à la fourniture de ce service) ;
- Lorsqu'une activité de traitement vise **plusieurs finalités**, le consentement doit être donné pour **toutes** ces finalités ;
- Le **retrait** du consentement doit être **aussi facile** qu'il est de le donner.

5. 10 étapes pour se mettre en conformité.

Le RGPD augmente considérablement les **exigences documentaires, organisationnelles et contractuelles** pour les organisations traitant des données à caractère personnel relevant du champ d'application de la législation européenne sur la protection de la vie privée.

Toutes les organisations devraient donc **vérifier avec une grande attention** que leur **structure actuelle, leurs processus opérationnels et leurs relations contractuelles** sont réellement conformes au nouveau cadre réglementaire.

Le **25 mai** prochain, c'est demain : il ne vous reste **plus beaucoup de temps** pour mettre en place les changements requis !

En nous inspirant des recommandations des institutions de l'Union européenne, et en accordant une attention particulière aux remarques du **Groupe de Travail de l'Article 29 (« A29 WP/G29 »)** et de différents superviseurs nationaux, nous avons **dressé une liste de 10 questions** pour vous aider à déterminer si les politiques et pratiques de votre entreprise en lien avec la protection de la vie privée nécessitent de quelconques améliorations.

Attention, chaque organisation étant **structurée** à sa façon et traitant des types de

données personnelles différents, cette liste doit être simplement considérée comme le point de départ d'une mise en conformité, sans se substituer à un **conseil juridique approprié**.

1 Gérez-vous des données personnelles relevant du RGPD ?

Tout d'abord, évaluez si votre organisation traite des informations personnelles concernant des personnes physiques identifiées ou identifiables, et si ces informations sont concernées par le droit de la protection de la vie privée de l'Union.

Si votre entreprise est établie dans l'UE, **la plupart** de ses activités liées au traitement des données personnelles est **susceptible** de tomber sous le champ d'application du RGPD.

Même si votre entreprise est établie en **dehors** de l'**UE**, le RGPD peut néanmoins s'appliquer sous certaines conditions, en particulier lorsque les données personnelles traitées **appartiennent** à des **individus résidant dans l'Union européenne**. Si votre réponse à la question posée en titre est « Oui », alors le RGPD s'applique : vous devriez soumettre votre organisation aux questions suivantes.

2 Traitez-vous des données personnelles de façon légale ?

Les **fondements** du traitement des données dans le cadre du RGPD ne diffèrent pas beaucoup de ceux déjà établis par la DPD. Il y a cependant **quelques variations**. Un point capital : le RGPD établit une norme plus élevée pour le consentement de l'utilisateur lorsque celui-ci est légalement requis pour traiter des données personnelles. En outre, comme nous l'avons précisé ci-dessus, il existe de nouvelles **limitations** concernant le **consentement des enfants**.

De façon générale, les responsables du traitement sont maintenant **expressément chargés** de démontrer qu'ils se conforment aux principes du droit à la vie privée et d'indiquer explicitement qu'ils doivent le faire (c'est le concept de la « reddition de comptes »).

3 Avez-vous mis à jour vos avis de pré information et vos politiques de confidentialité ?

Même lorsqu'une organisation est légalement autorisée à traiter des données personnelles, il existe de nombreuses obligations et exigences (dont certaines sont **nouvelles**). En conséquence, toutes les organisations sont tenues de **revoir** leurs politiques de protection des données, leurs pratiques internes et leurs procédures de formation afin d'assurer la conformité avec le RGPD.

Etant donné que le RGPD **élargit** les **informations** et les **droits d'accès** des détenteurs de données personnelles, la plupart des entreprises devraient revoir et mettre à jour leurs **notices d'information écrites** et **la politique de protection des données à caractère personnel de leurs sites web** afin d'éviter toute violation du nouveau cadre juridique.

Le RGPD exige des entreprises numériques qu'elles expliquent leurs droits de manière claire et transparente à leurs utilisateurs et clients. Le mot **« Transparence »** s'impose de plus en plus comme un mot-clé du nouveau cadre juridique.

4 Qui fait quoi en matière de protection de la vie privée dans votre organisation ?

Plus que jamais, on attend des entreprises concernées par le RGPD qu'elles mettent en place des **mesures de gouvernance** appropriées en matière de protection des données. Plus particulièrement, les responsables du traitement doivent prouver qu'ils ont implémenté les mesures techniques et organisationnelles appropriées pour s'assurer que les données personnelles sont traitées conformément au RGPD.

Votre entreprise doit allouer un budget approprié pour la conformité de la protection des données. En outre, des registres détaillés des activités de traitement des données personnelles devront toujours être conservés.

Il sera donc très important d'attribuer des **rôles** et des **responsabilités clairs** aux membres de votre organisation qui sont **impliqués** dans le traitement des données personnelles. Les cadres et les membres du personnel doivent être informés en permanence (grâce à des outils appropriés) des dernières directives publiées par l'autorité nationale de surveillance sur les questions de confidentialité.

5 Avez-vous besoin de nommer un Délégué à la Protection des Données ?

Le Délégué à la Protection des Données (DPD) est responsable de l'ensemble des questions relatives à la protection des données personnelles dans l'organisation.

Dans le cadre du RGPD, la désignation d'un DPD devient obligatoire pour une organisation dans trois cas spécifiques :

a. si le traitement des données est effectué par une **autorité ou un organisme public** (**quelles que soient** les données traitées) ; et/ou

b. lorsque l'une des **principales activités** du responsable du traitement ou du sous-traitant consiste en des opérations de traitement **exigeant un contrôle régulier**

et systématique des personnes concernées à grande échelle ; et/ou

c. lorsque l'une des principales activités du responsable du traitement ou du sous-traitant consiste au traitement **à grande échelle de catégories spéciales de données (données sensibles) ou de données personnelles relatives à des condamnations pénales et à des infractions.**

Alors qu'il est relativement facile de se positionner par rapport au cas (a), il n'est pas nécessairement simple de déterminer si l'organisation entre dans les catégories (b) et (c) – étant donné que le sens des termes « *principales activités* », « *grande échelle* » et « *contrôle régulier et systématique* » employés par le RGPD n'est pas défini par la loi.

Selon le groupe de travail G29, les « *principales activités* » devraient être comprises comme les tâches-clé nécessaires à l'atteinte des objectifs de l'organisation, y compris toutes les activités où le traitement des données forme une part inextricable de l'activité du responsable du traitement ou du sous-traitant. Par exemple, le traitement des données liées à santé est l'une des activités principales d'un hôpital, qui doit donc désigner un DPD.

Au contraire, le simple traitement des données personnelles des employés d'une organisation (par exemple, pour la paie) constitue une **activité accessoire** et non une activité principale de cette organisation, qui n'a donc aucune obligation de désigner un DPD.

Selon le groupe de travail G29, la notion de « *contrôle régulier et systématique des personnes concernées* » comprend toutes les formes de **suivi** et de **profilage sur Internet**, y compris à dans le but de faire de la publicité comportementale. D'autres **exemples** de « contrôle régulier et systématique » comprennent **l'email retargeting** et les **activités de marketing basées sur les données** ; le profilage et la notation à des fins d'évaluation de la solvabilité, le suivi de localisation par des applications mobiles, la **vidéosurveillance** (CCTV) et d'**autres appareils**.

L'organisation doit également considérer les facteurs suivants pour déterminer si son traitement des données est réalisé à « grande échelle » : le nombre de sujets concernés, le volume de données personnelles et/ou la gamme de données personnelles traitées ; la durée, ou la permanence, de l'activité de traitement des données ; l'étendue géographique de l'activité de traitement, etc.

Parmi les exemples de traitements à grande échelle mentionnés par le groupe de travail G29 : une compagnie d'assurance ou une banque traitant des données clients dans le cours normal de son activité ; les fournisseurs de téléphonie et d'accès à internet traitant certaines données (contenu, trafic, localisation) ; le traitement en temps réel des données de géolocalisation des clients d'une chaîne de fast-food internationale (opéré par un sous-traitant spécialisé) à des fins statistiques.

Attention, les **lois nationales** pourraient exiger de votre organisation qu'elle désigne un DPD dans d'autres **situations**.

Lorsqu'elle désigne un DPD, l'entreprise doit veiller à ce que ses autres tâches et fonctions n'entraînent pas de **conflit d'intérêts**. Le DPD ne devrait notamment pas occuper de poste lui permettant de déterminer les finalités / moyens du traitement des données personnelles (responsable des RH ou de l'informatique, par exemple) : cela mènerait inévitablement à un conflit d'intérêts.

Même si le RGPD n'exige pas la nomination d'un DPD dans une organisation donnée, celle-ci peut choisir d'en désigner un de façon volontaire. Dans ce cas, cependant, il sera expressément appliqué les mêmes exigences strictes du RGPD au DPD volontaire qu'aux DPD obligatoires.

6 Êtes-vous tenu de réaliser une Analyse d'Impact sur la Protection des Données (DPIA) ?

Selon le RGPD, lorsque les activités de traitement sont « susceptibles de présenter un risque élevé » pour les droits de protection des données, le responsable du traitement est **tenu** de procéder à une analyse préliminaire de l'impact des opérations de traitement qu'il envisage sur la protection des données personnelles.

On appelle ce processus d'évaluation la **DPIA (Data Protection Impact Assessment** ou Analyse d'Impact sur la Protection des Données).

Une DPIA est un **outil** fondamental pour se conformer aux exigences du RGPD et pour prouver que les mesures appropriées ont été mises en œuvre pour l'être. Elle est si utile que de nombreuses entreprises en ont déjà mené une, même dans les cas où elle n'était pas obligatoire.

Le groupe de travail G29 a tenté de **définir** quand les activités de traitement deviennent « susceptibles de présenter un risque élevé » pour les droits et libertés des personnes, et doivent donc être soumises à une DPIA.

L'organisation doit tenir compte des principaux facteurs suivants :

- L'évaluation ou la notation (y compris le profilage et la prédiction) notamment en termes de performance au travail, de situation économique, de santé, de préférences ou d'intérêts personnels, de fiabilité dans le comportement, de localisation ou de mouvement ;
- La prise de décision automatisée avec un effet juridique significatif ou d'importance similaire ;
- Le contrôle systématique ;

- Le traitement de données sensibles ou de données de nature très personnelle ;
- Le traitement de données traitées à grande échelle ;
- L'association ou la combinaison d'ensembles de données ;
- Le traitement de données concernant des individus vulnérables ;
- L'utilisation ou l'application innovantes de nouvelles solutions technologiques ou organisationnelles ;
- Lorsque le traitement en lui-même empêche les individus d'exercer un droit ou d'utiliser un service ou un contrat.

Sur la base des critères ci-dessus, le groupe de travail G29 a énuméré quelques exemples d'activités exigeant de réaliser une DPIA : la collecte de données issues des médias sociaux publics pour générer des profils, une organisation surveillant systématiquement les activités de ses employés (par exemple leur poste de travail, leur activité sur Internet, etc.) ; une institution financière créant une cote de crédit à grande échelle ou une base de données sur les fraudes…

La DPIA devrait au moins :

- décrire les opérations de traitement envisagées et leurs finalités ;
- analyser la nécessité ou la **mise en balance** du traitement par rapport aux risques qu'il présente pour les droits de protection des données ;
- lister les mesures envisagées pour gérer de tels risques et démontrer le respect du RGPD.

Si votre organisation conclut qu'une DPIA n'est **pas** requise, elle doit conserver les preuves des faits et des considérations qui ont mené à une telle conclusion.

7 Votre organisation est-elle prête à prendre les mesures requises par le RGPD ?

Le RGPD est susceptible d'augmenter les interactions entre les responsables du traitement et les personnes concernées, les autorités de surveillance ainsi que d'autres partie-prenantes. Dans le même temps, les entreprises seront régulièrement confrontées à des situations leur rappelant l'obligation à se conformer aux exigences du RGPD.

Par exemple, la plupart des responsables du traitement devront pouvoir répondre à des **demandes de portabilité des données** de la part

des personnes concernées. En cas de demande, vous devrez donc être en mesure de transmettre leurs données personnelles aux personnes concernées ou à d'autres responsables du traitement dans un **format approprié** et dans un **court délai**.

De plus, subsiste le problème des **violations des données**. Malheureusement, les **failles** de sécurité conduisant à la **perte ou à la divulgation non-autorisée de données personnelles** peuvent arriver à quasiment n'importe quelle organisation.

Le RGPD introduit une **obligation** de notifier la **violation des données** tant pour les responsables du traitement que pour les sous-traitants. Dans l'éventualité d'une violation des données personnelles, les sous-traitants sont tenus d'informer les responsables du traitement. Dans la plupart des cas, ces derniers doivent à leur tour **informer l'autorité de surveillance** compétente mais également, dans des **cas spécifiques**, les titulaires des données personnelles **concernés**.

8 Devriez-vous adhérer à un code de conduite ou demander une certification ou un label de protection des données ?

Le RGPD encourage l'approbation par les autorités nationales de surveillance de **Codes de Conduite** pour le traitement des données conforme aux règles du RGPD, qui seraient rédigés par des associations ou d'autres organismes représentant les responsables du traitement et les sous-traitants. Les organismes certifiés **contrôleront** qu'une organisation est conforme au Code de Conduite.

Lorsqu'un projet de Code de Conduite concerne des activités de traitement intra-européennes, une approbation préalable du Comité Européen de la Protection des Données sera requise. Si un tel Code de Conduite est approuvé, la CE pourra déclarer sa validité générale en **Europe**.

De plus, le RGPD encourage chaque Etat-membre à établir des **mécanismes de certification** en matière de protection des données ainsi que des **labels** ou des **marques** dans le but de démontrer plus facilement la conformité des acteurs avec le RGPD. Ces certifications, labels ou marques seront délivrés par des organismes accrédités dans chaque Etat de l'Union, ils ne dureront **pas plus** de **3 ans**.

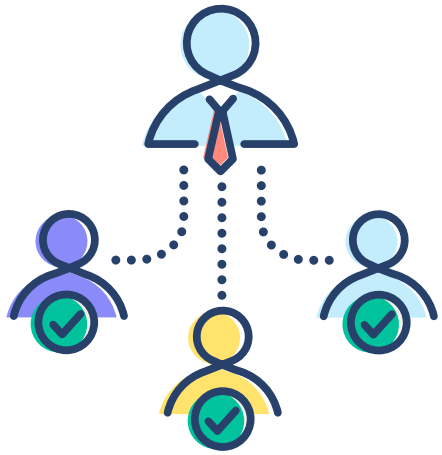
Cependant, dans le cas d'un **audit** mené par l'autorité de surveillance compétente, les organisations ayant reçu une certification devront **tout de même** prouver leur entière conformité avec le RGPD.

9 Vos « partenaires » sont-ils conformes au RGPD ?

Dans certaines conditions, une organisation peut être rendue **responsable** des violations du RGPD par des **tiers**, et notamment ses partenaires. Cela peut notamment arriver lorsqu'un responsable du traitement délègue le traitement des données

personnelles à un **sous-traitant non conforme** ou lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement des données personnelles.

Lorsqu'un responsable du traitement confie à un sous-traitant des activités de traitement, le RGPD souligne les exigences suivantes :



- le sous-traitant fournit suffisamment de garanties concernant le fait qu'il met en place les mesures techniques et organisationnelles nécessaires pour satisfaire aux exigences du RGPD (et si ce n'est pas le cas, les deux parties peuvent être tenues conjointement responsables des infractions à la loi sur la protection des données) ; et
- les activités du sous-traitant et sa relation avec le responsable du traitement doivent être régies par un contrat.

En outre, lorsque cohabitent des **responsables du traitement conjoints** dans le cadre du traitement spécifique de données personnelles, ils doivent consigner leurs rôles et responsabilités respectifs relatifs au RGPD dans un **accord écrit**. L'essentiel de l'arrangement doit être mis à la **disposition** des détenteurs des données personnelles.

À la lumière de ce nouveau cadre juridique, la plupart des organisations doivent revoir et mettre à jour les **clauses de confidentialité** de leurs **outils contractuels**, tant avec leurs **clients** qu'avec leurs **fournisseurs**, afin d'éviter toute responsabilité auprès de tiers.

10 Transférez-vous des données personnelles en dehors de l'Espace économique européen (EEE) ?

Suivant les mêmes orientations que la DPD, le RGPD impose des **restrictions** importantes au **transfert** de données à caractère personnel de **l'EEE** vers des **pays tiers** (ou des **organisations internationales**). La raison à cela, c'est que tous les pays ou territoires ne garantissent pas un niveau adéquat de protection des données personnelles.

Dans le cadre du RGPD, le transfert de données personnelles vers un pays tiers (ou vers une organisation internationale) n'est autorisé que si au moins l'une des conditions suivantes est remplie :

- La **CE** a **décidé** que ce pays assure un niveau de protection adéquat (la liste des pays « adoubés » par la CE dans le cadre de la DPD sera toujours valable) ;

- Le responsable du traitement ou le sous-traitant du pays tiers a fourni des **« *garanties appropriées* »,** mais toujours à la condition que les droits applicables sur la protection des données et des recours légaux efficaces soient disponibles. Selon le RGPD, les « garanties appropriées » **incluent** : des règles d'entreprise contraignantes ; des clauses types de protection des données adoptées par la CE ; des clauses types de protection des données approuvées par la CE et adoptées par une autorité de contrôle ; des Codes de Conduite ; des mécanismes de certification (sous certaines conditions).

Les autres principales **dérogations** à la restriction du transfert de données personnelles en dehors de l'EEE sont fondées sur les motifs suivants :

- Le consentement éclairé de la personne concernée ;
- Une nécessité contractuelle ;
- Des raisons importantes d'intérêt public ;
- La constatation, l'exercice ou la défense d'un droit en justice ;
- Les intérêts vitaux de la personne concernée ou d'autres personnes ;
- Des données du registre public.

6. Les avantages à vous conformer au RGPD.

Le RGPD vise essentiellement à protéger la vie privée des individus, et pas nécessairement à défendre l'intérêt des entreprises. De plus, les nouvelles réglementations augmentent clairement le temps et les coûts consacrés à se conformer à la loi et à former les équipes de façon adéquate. C'est pourquoi le RGPD n'est pas forcément perçu par les entreprises comme une bonne nouvelle.

Et pourtant, en se conformant aux nouvelles règles, la plupart des entreprises en tirera des bénéfices à plusieurs points de vue :

- **Réputation :** une sécurité renforcée améliorera la réputation et la crédibilité de votre entreprise tant auprès de vos partenaires que de vos clients. Au contraire, les cyberattaques ou les violations de données peuvent facilement ternir la réputation d'une organisation ; sans compter les plaintes des clients sur Internet (médias sociaux, etc.), qui peuvent avoir un effet dévastateur sur votre image de marque.
- **Des données marketing plus précises et efficaces :** dans le cadre du RGPD, les marketeurs seront uniquement autorisés à utiliser les données personnelles des utilisateurs qui y ont donné leur accord. Cela signifie des bases de données utilisateurs plus minces mais de meilleure qualité avec, au moins à moyen

terme, des taux de conversion plus élevés pour les campagnes marketing. Les organisations seront ainsi de plus en plus tenues de maintenir les données personnelles de leurs utilisateurs / clients correctes et à jour, avec des effets bénéfiques significatifs lors de la transformation de ces données en chiffres de ventes.

- **Conséquences juridiques :** ce que vous dépensez aujourd'hui en conseils juridiques et en audit interne pourrait un jour vous éviter des lourds dommages ou pénalités : la pleine conformité avec le RGPD vous permet d'éviter les potentielles responsabilités civiles et leurs conséquences administratives ou pénales.

Contacts.

Vous souhaitez prolonger la discussion ? Contactez-nous !

Alan Rhode
Co-fondateur de Taxmen
Alan.rhode@taxmen.eu

Sandra Fernandes
Directrice Marketing et Communications chez Splio
sfernandes@splio.com

À propos de Taxmen

Taxmen was established in 2012 to provide one-stop-shop compliance services for VAT on distance selling and environmental regulations on e-commerce packaging in all the European jurisdictions. It has subsequently widened its tax activities, which now range from customs law advise to advise relating to WEEE. From 2014, the company provides legal services specifically tailored for the IT sector under the brand Lawmen.

www.taxmen.eu

À propos de Splio

Splio édite une plateforme omnicanale qui, basée sur la connaissance client, associe marketing automation et marketing de fidélisation, pour permettre aux marketeurs d'aligner leur stratégie de communication on et offline, d'offrir des expériences clients fluides et connectées, et de générer ainsi du chiffre d'affaires.

Basée à Paris, Splio a des bureaux en Chine, Espagne, Italie, Pologne, et Brésil, et compte plus de 500 clients, parmi lesquels The Kooples, Kusmi Tea, Givenchy, Caudalie, Degrenne, Desigual, Lindt, Air China et Cache Cache.

www.splio.com

Splio

TAX MEN LAW MEN
TAX & LEGAL FOR E-COMMERCE