Marketing et RGPD

Les 15 questions les plus posées,
un an après

qualifio

Introduction

Comment recueillir le **consentement** ? Qu'en est-il des données récoltées dans le cadre des **réseaux sociaux** ? Et sous quelles conditions peut-on envoyer des sollicitations commerciales ? Les avocats du cabinet Lex4U répondent aux questions les plus posées par les professionnels du marketing, un an après la mise en application du RGPD.

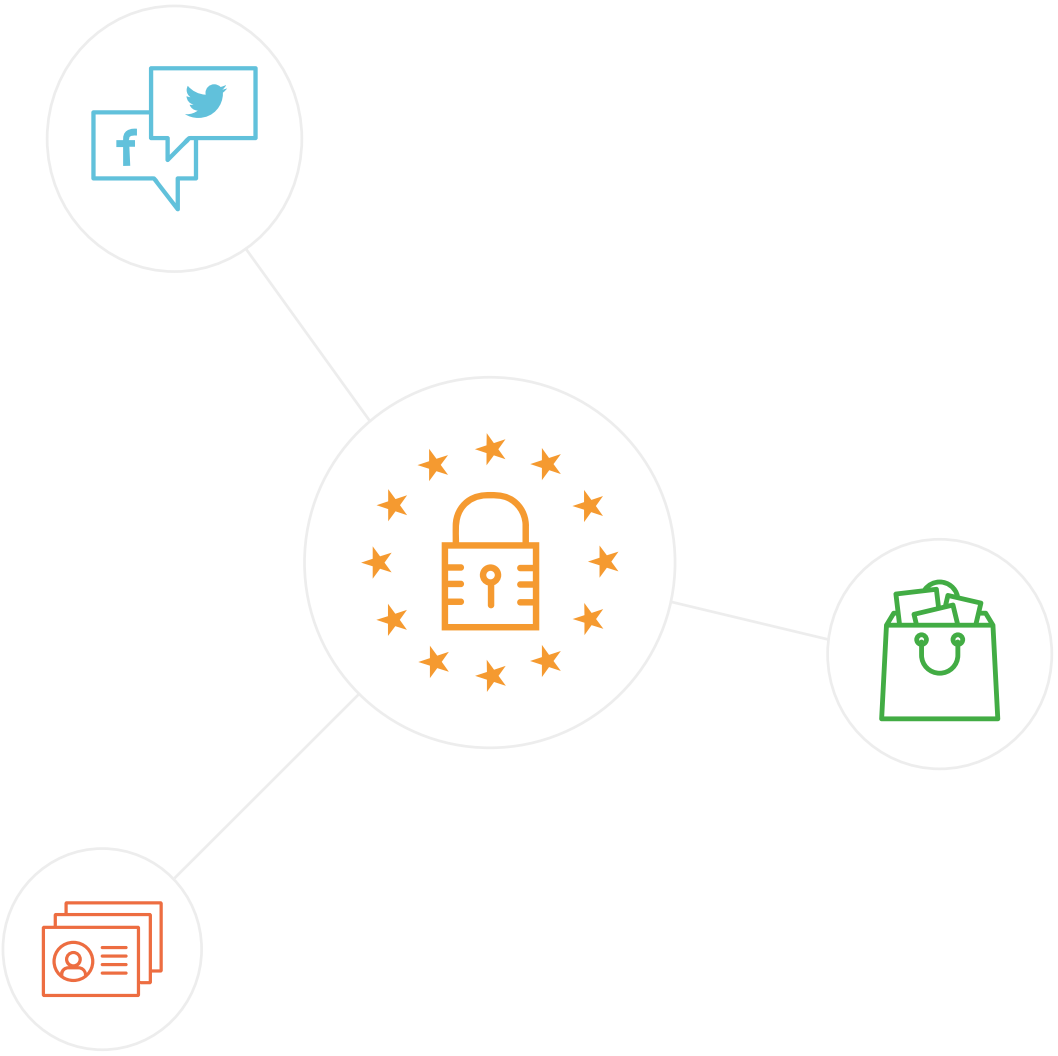


Table des matières

1 Comment recueillir le consentement ?

Au niveau du RGPD, le consentement n'est pas à prendre à la légère. Une simple case à cocher peut faire l'affaire, dans certains cas, pour autant qu'il soit mentionné de manière spécifique à quel traitement ce consentement est lié. Par exemple, « j'accepte de recevoir des offres commerciales de la société X. » Il devra également faire mention d'un lien vers la Politique Vie Privée, pour que le prospect sache à quoi vont servir ses données personnelles.

Ce consentement doit donc présenter plusieurs caractéristiques. Il doit être :

LIBRE : le consentement doit bien sûr être donné librement. Aucune pression ne peut être exercée sur la personne concernée. C'est pourquoi le consentement ne sera pas considéré comme « libre » s'il y a déséquilibre entre la personne et le responsable du traitement des données. Exemples de déséquilibre : un citoyen par rapport à l'autorité ou un travailleur par rapport à son employeur.

SPÉCIFIQUE : Le consentement ne peut être lié qu'à une ou plusieurs finalités qui doivent être clairement définies. Par exemple, dans le cas où vous proposez plusieurs newsletters, un consentement donné pour un envoi de newsletter liée aux voitures ne peut être entendu comme un consentement pour l'envoi d'une newsletter relative à l'immobilier.

ÉCLAIRÉ : lorsque vous demandez le consentement, celui-ci doit être formulé en des termes clairs et simples, et exprimer des informations compréhensibles et accessibles. Il n'est donc pas conseillé d'utiliser du jargon juridique ou technique, qui sera bien souvent incompréhensible par votre prospect.

UNIVOQUE : la personne concernée doit comprendre que son consentement vous autorise à utiliser ses données à caractère personnel.

ATTENTION

Le recueil du consentement par l'acceptation des conditions générales d'utilisation ou de vente n'est pas valable. Veillez donc à créer un *opt-in* supplémentaire qui vous aidera à recueillir ce consentement en bonne et due forme car l'information liée aux données personnelles ne peut se confondre avec d'autres informations.

2 Comment envoyer des sollicitations commerciales par voie électronique, sans enfreindre le droit à la vie privée, dans une relation B2C ?

Avant de répondre à cette question, il est bon de rappeler la différence entre marketing postal, téléphonique et digital.

La différence majeure est qu'il n'est **pas nécessaire de recueillir le consentement dans le cadre d'un appel téléphonique avec intervention humaine** (à l'opposé d'un système automatisé de communication électronique) **ou de l'envoi de courrier postal**, pour autant que la personne contactée ait été correctement informée et qu'elle n'ait pas fait usage de son droit d'opposition.

En outre, il est possible d'envoyer un e-mail de prospection commerciale à un particulier sans son consentement préalable si cette prospection concerne un produit ou un service analogue et que cette personne a été informée de l'utilisation de ses données à des fins de prospection commerciale.

Il est cependant **essentiel de recueillir ce consentement dans le cadre d'une communication digitale** (via e-mail, fax ou texto) et de permettre au destinataire de faire usage de son droit d'opposition de manière simple.

Dans tous les cas, selon les règles du RGPD, le responsable du traitement des données se doit de donner les informations les plus claires possibles sur l'utilisation de celles-ci, pour des sollicitations commerciales et caritatives des campagnes marketing direct.

Afin de recueillir ce consentement, nous vous conseillons l'utilisation d'un ***opt-in***, c'est-à-dire une case à cocher expliquant pour quelle finalité vous souhaitez collecter les données de la personne.

LES CONSEILS DU PRO

- Évitez de collecter des adresses e-mails de particuliers sur des sites ou des forums de discussion ;
- Ne pré-cochez pas les cases lorsque vous demandez à une personne d'accepter de recevoir des communications commerciales ou des communications de la part d'autres partenaires ;
- Ne conditionnez pas l'accès à un service, l'achat d'un bien ou le bénéfice d'une réduction à l'acceptation de recevoir des messages publicitaires par voie électronique.

3 Comment envoyer des sollicitations commerciales par voie électronique, sans enfreindre le droit à la vie privée, dans une relation B2B ?

Comme dans le B2C, au moment de la collecte de données, la personne doit être **informée** que son adresse e-mail sera utilisée à des fins de prospection commerciale. Elle doit également être, à tout moment, **en mesure de s'opposer** à ce type d'utilisation simplement et gratuitement.

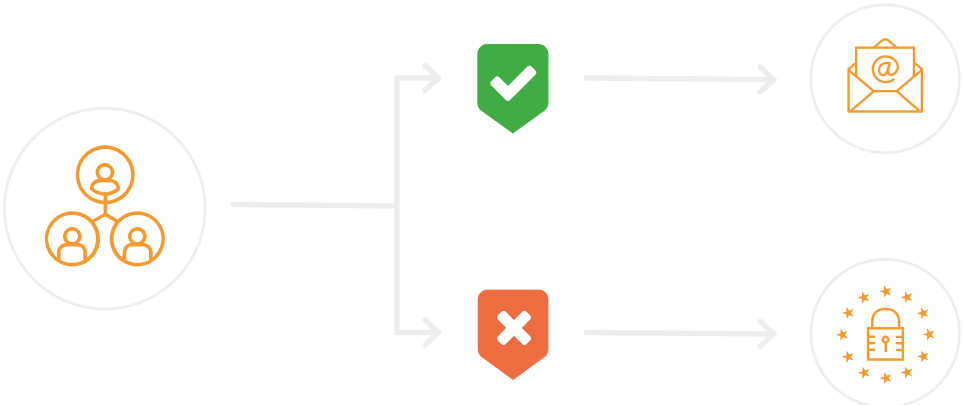
ATTENTION

L'objet de la sollicitation doit être en rapport avec la profession du professionnel.

Peut-on envoyer des e-mails aux adresses info@ ou contact@ ?

Les adresses professionnelles génériques, par exemple info@ ou contact@, ne sont pas soumises aux principes de consentement et d'opposition car il ne s'agit pas de données à caractère personnel.

La question devient discutable à partir du moment où l'adresse e-mail contient le nom et le prénom de la personne. Dans ce cas, l'adresse e-mail contient des données à caractère personnel. Les principes de consentement et d'opposition s'appliquent donc.



4 Dans quels cas ne faut-il pas recueillir de consentement ? Quelles sont les exceptions ?

Il existe deux cas dans lesquels il ne faut pas recueillir de consentement :

1

Si le message commercial est envoyé sur l'adresse e-mail professionnelle d'une personne physique et que l'objet du message est en rapport avec sa profession. Comme nous l'avons vu dans la question précédente, nous sommes alors dans un cadre B2B. Il convient néanmoins d'informer la personne lors de la collecte de son adresse e-mail.

2

Le message commercial concerne des produits ou services similaires ou analogues à ceux que le consommateur a déjà acquis auprès de la même entreprise. Encore une fois, cette personne doit être informée du fait que ses coordonnées seront utilisées à des fins de prospections commerciales, mais uniquement pour des produits ou services analogues à ceux déjà fournis par la même entreprise.

Il est également important que la personne soit en mesure de pouvoir s'opposer à l'utilisation de ses données.

5 Qu'est-ce que le droit d'opposition dans le RGPD ?

Le RGPD confère à la personne **le droit de s'opposer au traitement de ses données personnelles**, notamment, lorsque ces dernières sont traitées à des fins de prospection. Par conséquent, toute communication commerciale par voie électronique doit offrir au consommateur un moyen de ne plus recevoir ce type de message de manière simple, gratuite et aisément accessible.

PAR EXEMPLE

Dans un e-mail publicitaire, il vous faudra prévoir un lien direct pour se désabonner du mailing/listing client, de manière claire et séparée de toute autre information.

Il est important de noter que ce droit d'opposition à la prospection commerciale doit être porté explicitement à la connaissance de la personne concernée. Une fois que la personne aura fait usage de son droit d'opposition, le responsable de traitement devra mettre en place les mesures nécessaires pour mettre un terme à ce traitement.

6 Est-il permis de réutiliser les données collectées à d'autres fins que celles pour lesquelles elles ont été initialement collectées ?

Non, il n'est pas possible de réutiliser ces données dès lors qu'elles ont été collectées pour une finalité particulière.

PAR EXEMPLE

Les coordonnées recueillies lors d'une opération de recrutement ne peuvent pas être utilisées pour adresser de la publicité. La personne qui a consenti à donner ses informations dans le cadre de ce recrutement n'a pas donné son autorisation à recevoir des communications commerciales.

7 Pouvez-vous transmettre les données collectées à des partenaires commerciaux ?

Il est possible d'adapter les modalités de recueil du consentement de façon à rendre cette transmission légale, mais cela nécessite plusieurs conditions :

➔ La personne doit donner son consentement avant toute transmission à des partenaires.

PAR EXEMPLE

Vous pourriez prévoir une case à cocher lors de la collecte des données avec la phrase « J'accepte de recevoir les offres des partenaires commerciaux » et rajouter un lien vers la liste des partenaires.

➔ Un certain nombre d'informations sur l'**identité des partenaires** doit être fournies à la personne concernée.

PAR EXEMPLE

Lors du recueil de consentement, une liste exhaustive des partenaires commerciaux doit être facilement accessible soit via le formulaire, soit via un lien. N'oubliez pas de renvoyer la personne concernée vers les Politiques Vie Privée des différents partenaires afin qu'elle soit bien informée du traitement de ses données par vos partenaires commerciaux.

➔ Il faut que la personne soit informée des **évolutions et modifications** de la liste des partenaires, en particulier lorsqu'il s'agit de l'arrivée de nouveaux partenaires.

Cela peut se faire de plusieurs façons : lorsque la société à l'origine de la collecte des données envoi un courriel de prospection, elle peut informer la personne des évolutions de la liste de partenaires. Et lorsque le nouveau partenaire souhaite communiquer pour la première fois avec la personne prospectée, il informe la personne concernée, dans un délai d'un mois, du traitement qu'il fait de ses données.

IMPORTANT

Le **consentement** que la société a recueilli pour collecter les données pour le compte de ses partenaires **n'est valable que pour ces derniers**. Ces partenaires devront recueillir le consentement de la personne s'ils souhaitent envoyer les données reçues à leurs propres partenaires. En d'autres termes, **il n'y a pas de transmission de ce consentement**.

➔ Les partenaires doivent veiller, dès la première communication avec la personne concernée, à lui **indiquer la source** par laquelle ils ont obtenus ses données et la manière dont la personne peut **exercer ses droits**. Enfin, ils doivent respecter les obligations d'information reprises à l'**article 14 du RGPD**.

➔ Le **droit d'opposition** s'exerce soit auprès du partenaire, soit auprès de la société à l'origine de la collecte initiale des données. Attention que dans le dernier cas, la société à la source de la collecte devra répercuter les effets de ce droit d'opposition auprès de ses partenaires qui sont également destinataires de ces données.

PAR EXEMPLE

Une personne exprime son souhait de s'opposer au traitement de ces données dans un but de prospection commerciale, directement auprès de la société qui a initialement collecté ses données. Cette société va devoir ensuite en informer ses partenaires à qui les données de la personne concernée ont été transmises. Il y a donc un travail de communication à faire du côté de la société à la source de la collecte de ces données afin de répercuter l'information.

Pour résumer, lors de la transmission de données à des partenaires commerciaux, il est indispensable d'informer sur :

- le nom de la société qui a transmis les données aux partenaires (société à l'origine de la collecte) ;
- l'identité des partenaires et une liste à jour de ceux-ci ;
- les finalités pour lesquelles les partenaires vont traiter ces données ;
- les droits des personnes concernées, et en particulier le droit de s'opposer à de la prospection commerciale de la part du ou des partenaires.

8 Qu'en est-il des pays hors de l'Union Européenne ?

Rappelons que le point central du RGPD est la **personne physique**, le citoyen européen. L'objectif étant de **protéger** les personnes contre les usages abusifs que les entreprises peuvent faire de leurs données. C'est pourquoi le RGPD s'applique également au-delà de l'UE.

Il faut donc comprendre que le RGPD s'applique même aux entreprises établies dans des pays tiers à l'UE **dès lors que le traitement des données personnelles porte sur un résident de l'UE**. En effet, que le traitement ait lieu ou non dans l'Union, le RGPD a une portée globale.

Le cas de la Suisse

Pour ce qui est de la Suisse, la Commission européenne a adopté une « décision d'adéquation ». Il s'agit d'une décision par laquelle la Commission reconnaît qu'un pays tiers à l'UE offre un niveau de protection des données à caractère personnel comparable à celui garanti dans l'UE. Grâce à cette « décision », les données à caractère personnel peuvent circuler entre l'UE et le pays tiers concerné.

Dès lors, les européens bénéficient d'un niveau de protection accru, conforme aux normes de l'UE en matière de protection de la vie privée, lorsque leurs données sont transférées vers la Suisse.

LISTE DES PAYS QUI ONT FAIT L'OBJET D'UNE DÉCISION D'ADÉQUATION

Andore, Argentine, Canada, Guernesey, Îles Féroé, Île de Man, Israël, Japon, Jersey, Nouvelle-Zélande, Suisse et Uruguay.

Le cas des États-Unis

Il n'y a pas de loi générale sur la protection des données aux États-Unis. Toutefois, un mécanisme d'auto-certification, plus connu sous le nom de *Privacy Shield* (ou Bouclier de Protection des Données) a été mis en place. Celui-ci a été reconnu par la Commission européenne comme offrant un niveau de protection adéquat aux données personnelles transférées vers les États-Unis.

EN QUELQUES MOTS

Le *Privacy Shield* est une décision d'adéquation « partielle », car le transfert des données n'est facilité que pour les entreprises qui se sont engagées à respecter ses principes.

Cependant, en juillet 2018, le Parlement européen a désavoué ce système en estimant que « *l'actuel Bouclier de Protection des Données n'offre pas le niveau de protection adéquat requis par le droit de l'Union en matière de protection des données et par la charte des droits fondamentaux de l'Union Européenne* ».

COMMENT S'ASSURER QUE LES DONNÉES TRANSMISES VERS LES ÉTATS-UNIS BÉNÉFICIENT D'UN NIVEAU DE PROTECTION ADÉQUAT ?

Si une société est auto-certifiée *Privacy Shield*, un transfert de données vers elle peut, à tout le moins pour le moment, être effectué. Cependant, en tenant compte du désaveu du Parlement européen, il conviendrait peut-être de prendre des précautions supplémentaires et d'organiser les transferts vers les USA sur base d'une des autres possibilités offertes par le RGPD.

De manière pratique, on pense directement à un contrat contenant les clauses contractuelles types qui ont été mises en place par la Commission européenne.

D'autres mécanismes existent dans le Règlement mais il convient de les utiliser avec parcimonie au regard soit de leur caractère restrictif (liste des dérogations), soit de la lourdeur de leurs mises en place (codes de conduite ou règles d'entreprise contraignantes).

Et le Brexit ?

L'impact qu'aura le Brexit sur l'application du RGPD au Royaume-Uni dépend des négociations politiques avant la date officielle du Brexit, fixée au 31 octobre 2019.

Il y a dès lors deux possibilités :

SOIT L'ACCORD AVEC L'UE EST APPROUVÉ

Dans ce cas, il y aura une période transitoire de deux ans au cours de laquelle le RGPD restera d'application. Rien ne changera donc durant les 2 années qui suivent le Brexit en ce qui concerne le transfert des données vers le Royaume-Uni.

SOIT L'ACCORD AVEC L'UE N'EST PAS APPROUVÉ

Sans accord, le Royaume-Uni sera considéré comme un pays tiers à partir du 1er novembre 2019. Il faudra alors pallier à l'absence d'accord grâce à l'un des outils permettant l'encadrement de ces transferts (une décision d'adéquation par exemple).

Cependant, avec la démission de Theresa May, on peut craindre le pire.

9 Qu'en est-il des données récoltées dans le cadre des réseaux sociaux ?

L'utilisation des données collectées via les réseaux sociaux est une question compliquée. Il faut donc faire attention à ne pas tomber dans la facilité : ce n'est pas parce que les données sont publiques qu'elles peuvent pour autant être utilisées librement.

Le cas de LinkedIn

Prenons un exemple simple : vous recherchez le moyen de contacter une personne sur LinkedIn et trouvez son adresse e-mail, publiée sur son profil. Celle-ci vous est accessible car vous faites partie de son réseau professionnel.

Selon les principes du RGPD, il vous faut une **base légale** pour l'utilisation de cette donnée personnelle. Dans le cadre du marketing direct, que ce soit en B2C ou en B2B, il convient d'informer la personne concernée quant à l'utilisation de ses données personnelles. Dans ce cas, même sur base de l'application de l'**article 14 du RGPD** mentionnant la possibilité de traiter des données que vous n'avez pas vous-même collectées, il vous sera compliqué d'expliquer que la personne concernée a été clairement informée au moment de la collecte.

À l'opposé, il sera plus aisé de justifier un contact vers une personne dans le cadre d'une sollicitation professionnelle, au vu des objectifs du réseau social LinkedIn.

Le cas des concours Facebook

Exemple : vous lancez un **concours pour les fêtes de Pâques** dans lequel vous invitez votre audience à trouver un oeuf caché dans l'une des publications de votre page Facebook.

Depuis l'**arrêt Wirtschaftakademie**, les gestionnaires de pages Facebook sont considérés comme co-responsables de cette page.

Afin de réutiliser les informations collectées dans le cadre de ces concours, il vous faudra informer correctement les participants sur le traitement de leurs données. Cette explication peut prendre place dans le cadre de votre politique vie privée, accessible via un lien, par exemple.

Enfin, il faudra respecter le principe de finalités et ne pas réutiliser les données de ces personnes pour une autre finalité, à moins que celle-ci ne soit compatible avec celle initiale, comme envisagé dans l'**article 6 (point 4) du RGPD**.

10 Quel est l'impact du RGPD sur le ciblage d'audience sur les réseaux sociaux?

Concernant le ciblage d'audience, la première question à se poser est évidemment « ce traitement permet-il d'identifier une personne physique ou de la rendre identifiable ? »

Si on parle d'un ciblage général (typiquement une tranche d'âge sur un territoire défini), il est impossible d'identifier précisément une personne physique sur base de ce seul ciblage.

Si, en revanche, le ciblage concerne une analyse comportementale en fonction des pages appréciées par la personne physique, ce ciblage est directement lié à son comportement propre. La société tierce souhaitant faire du marketing en utilisant cette donnée comportementale devra alors s'assurer que Facebook a bien recueilli le consentement de la personne physique.

Évidemment, dans le cas repris ci-dessus, il conviendra d'accorder une importance fondamentale à l'information prodiguée à la personne physique, tant de la part de Facebook que de la société traitant ces données.

Au regard des différentes décisions concernant Facebook, rendues par les différentes autorités européennes, il s'agira d'être extrêmement prudent.

Concernant les traceurs et *retargeting*, le sujet est en vogue. En effet, l'Avocat Général Michal Bobek a rendu des conclusions générales dans le cadre de l'affaire FASHION ID qui, de manière schématique, pourraient amener à considérer que le gestionnaire d'un site web est co-responsable de traitement de la société qui a installé le plugiciel.

11 Qu'en est-il du stockage et de la rétention des données ?

Il est important d'adopter des comportements logiques en matière de stockage et de rétention des données, et en matière de sécurité surtout.

Sécurité physique

Un exemple commun est celui des **armoires non fermées à clé**.

Imaginez : vous travaillez dans un bureau comptable. Vous accueillez un client dans votre bureau et partez dans une autre pièce, le laissant seul face à une armoire ouverte. Dans cette armoire se trouvent des dossiers d'autres clients, contenant les données à caractère personnel. Il existe un risque que votre client, laissé seul, accède à ces données.

Il est, bien entendu, important de **mettre vos dossiers en sécurité en toutes circonstances**. Veillez donc à fermer vos armoires à clé.

Sécurité informatique

Il en est de même lorsque l'on parle d'informations digitales. L'une des bonnes pratiques de sécurité informatique est de mettre en place des **codes d'accès** au serveur de votre entreprise, ainsi qu'un **identifiant unique** par personne.

!

ATTENTION

La sécurité informatique est le terrain de prédilection de la **CNIL** (Commission Nationale Informatique et Libertés). Pensez donc à une bonne sécurité pour vous mettre à l'abri des sanctions.

Exemple : Grand Optical

La CNIL a condamné Grand Optical France à une amende de 250.000 € pour avoir insuffisamment sécurisé les données de ses clients effectuant une commande en ligne à partir de son site internet.

Il était en effet possible d'accéder à des centaines de factures de clients de la société via le site internet de Grand Optical France. Ces factures contenaient des données telles que les noms, prénoms, adresses postale ainsi que des données de santé (correction ophtalmologique) ou encore, dans certains cas, les numéros de sécurité sociale des personnes concernées.

La CNIL a constaté un défaut de sécurité. En effet, le site www.opticalcenter.fr n'intégrait pas de fonctionnalité permettant de vérifier qu'un client est bien connecté à son espace personnel (« espace client ») avant de lui afficher ses factures.

12 Où en est-on sur les sanctions ?

Des sanctions et des contrôles ont déjà été mis en place dans plusieurs pays, dont la France. L'Autorité de Protection des Données française sanctionne tant les grandes entreprises, comme Google, que les plus petites.

L'exemple Google

Google a été sanctionné d'une amende de 50 millions d'euros pour son **manque de transparence et d'information**. Il a été jugé que les informations communiquées par Google n'étaient pas aisément accessibles pour les utilisateurs et ne sont pas systématiquement claires et compréhensibles. Les utilisateurs n'étaient pas en mesure de comprendre les traitements dont leurs données personnelles font l'objet.

L'exemple d'une société immobilière

Une sanction pécuniaire a également été prononcée par l'Autorité de Protection des Données française à l'encontre d'une société immobilière qui avait démarché, par texto et **sans leur consentement**, des propriétaires de biens immobiliers à vendre.

Il n'y a donc pas que les grandes entreprises qui sont soumises au contrôle des autorités et aux sanctions.

Et en Belgique ?

Du côté belge, l'Autorité de Protection des Données belge a également commencé ses premières réunions, et donc ses premiers contrôles. **Il ne faut donc pas lésiner sur votre mise en conformité** en matière de protection des données car les conséquences en cas de non-respect peuvent s'avérer lourdes.

13 Comment traiter les informations récupérées lors d'évènements ?

1er cas : les données sont récupérées par l'orateur

L'orateur d'une conférence obtient la liste des personnes présentes ainsi que leurs adresses e-mails, via lesquelles elles se sont inscrites.

Une bonne pratique serait qu'au moment de l'inscription, les personnes concernées soient informées de la transmission de la liste à l'orateur et des finalités pour lesquelles il va traiter ces données personnelles.

Mais quelle est la base légale appliquée ?

- Lors de l'inscription, un *opt-in* spécifique est prévu et les finalités clairement définies dans le message de l'*opt-in*. Cela permet alors de traiter les données sur base d'un consentement.
- Base légale de l'intérêt légitime : dans ce cas, il faudra informer correctement et préalablement les personnes concernées. Vous devrez aussi leur laisser la possibilité, le jour-même et après, de s'opposer au traitement de leurs données personnelles à des fins marketing.

2e cas : les données sont récupérées via une application

Imaginez : vous êtes présent à un salon de l'auto. Le salon a mis en place une application dans laquelle les personnes présentes peuvent mettre des données personnelles telle que leurs noms, prénoms, dates de naissance et adresses e-mail. Ces données créent un **QR code unique** qui est relié à l'adresse e-mail de la personne concernée.

En tant qu'exposant vous avez aussi accès à l'application mais vous avez une fonctionnalité permettant de scanner le QR Code afin d'obtenir l'adresse e-mail, le nom et le prénom de la personne qui passe par votre stand.

COMMENT TRAITER LES DONNÉES ?

- Il convient de **vérifier que le salon organisateur qui a mis en place un document relatif à la vie privée** accessible via l'application et qui explique les tenants et les aboutissants des traitements de données qu'il effectue. En outre, il convient de vérifier que ce document d'information parle et explique clairement que le fait de scanner le QR code va transférer les données à un exposant donné.
- En votre qualité d'exposant, vous pourrez contacter la personne qui s'est présentée à votre stand - dans le cas où la personne vous a présenté son téléphone avec le QR Code de son plein gré. Vous devrez pour cela respecter les prescrits de l'**article 14 du RGPD** dès lors que vous n'avez pas collecté les informations de la personne concernée vous-même.
- **Contextualisez votre premier contact** avec une phrase simple et claire, comme « Nous nous sommes rencontrés dans le cadre du salon X. »
- Au niveau de la **base légale**, il est possible de justifier ces traitements sur base de l'intérêt légitime. La personne a effectivement eu l'air intéressée par vos services sinon elle ne vous aurait pas montré son QR Code à scanner. C'est pourquoi il est extrêmement important de vérifier les documents légaux qui sont utilisés par ce genre d'application afin de vérifier que la personne concernée a été informée correctement de l'utilisation que vous comptez en faire.

3e cas : l'exemple de Batibouw

Imaginez : vous rencontrez un prospect au salon Batibouw (salon immobilier). Votre société, spécialisée en salle de bains et de cuisines, fait une première estimation sur base des explications et demandes de ce prospect.

Suite à ce premier contact, vous le contactez la semaine d'après. Vous utilisez donc la base légale de la nécessité à l'exécution d'un contrat, et plus précisément aux mesures précontractuelles.

Finalement, après un devis plus complet, la personne concernée ne souhaite pas donné suite à ce devis.

Que faire de ces données personnelles ? **Rien**.

En effet, la personne vous a donné ses données pour une finalité précise : la construction d'une cuisine. Elle ne vous a pas autorisé à utiliser ses données pour d'autres finalités.

Une bonne pratique serait de prévoir des formulaires de devis avec des *opt-in* permettant de prendre le consentement de la personne concernée pour d'autres finalités que celle liée à la vente, notamment celle d'envoi de documentation relative à la prospection commerciale.

14 Que se passera-t-il en matière de RGPD et d'*e-Privacy* dans le futur ?

Le futur est, par principe, incertain. Il n'est pas aisé de prévoir ce qui va se passer. Cependant, voici quelques pistes de réflexion :

- On peut évidemment s'attendre à ce que **d'autres sanctions tombent**, en particulier en Belgique où l'Autorité de Protection des Données a récemment tenu ses premières réunions qui découleront donc, probablement, sur des premiers contrôles.
- La **décision d'adéquation** récente concernant le Japon nous amène à penser que la Commission va tenter d'étendre les échanges internationaux avec de nouveaux accords du même type, ceux-ci favorisant évidemment les échanges commerciaux.
- Et enfin, toujours dans une perspective de renforcement du marché unique numérique, **une proposition de règlement *e-Privacy***, concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques, a été déposée pas encore adopté. Il devait, à la base, entrer en vigueur en même temps que le RGPD.
- Ce règlement complète et précise le RGPD : il vient renforcer les obligations de respect de la vie privée et de confidentialité des communications dans le secteur des communications électroniques. Il permettra d'harmoniser toutes les lois nationales dans l'UE concernant ce type de communication et impactera directement le marché du marketing digital.

15 Comment motiver les consommateurs à consentir à partager leurs données ?

La question de la motivation est sans doute la plus difficile de toutes. Comment les motiver à partager leurs données personnelles ? Deux exemples :

Ayez une bonne Politique Vie Privée

De manière générale, la mise en place d'une bonne politique vie privée, d'une **information claire et transparente sur la manière dont sont traitées les données**, suscite la confiance dans le chef des consommateurs.

Pour la plupart, les consommateurs sont craintifs car ils ne comprennent pas ce à quoi ils s'engagent lorsqu'ils transmettent leurs données.

Il faut donc leur donner la possibilité de se renseigner au préalable de manière très **transparente**, les utilisateurs doivent être en mesure de comprendre les traitements dont leurs données à caractère personnel font l'objet.

Vers la monétisation du partage de données

Au Japon, par exemple, il est possible de payer votre consommation en échange de vos données personnelles.

Une chaîne japonaise propose aux étudiants de payer leurs cafés en fournissant des données personnelles. Ces données sont ensuite transmises à des entreprises partenaires. Ces sont ces entreprises « sponsors » qui paient le café en échange de sondages ou d'autres sollicitations.

En contrepartie, les étudiants recevront des publicités ou des sondages à remplir.

Privilégiez les contenus interactifs et la collecte de données « first-party »

Si vous êtes un(e) professionnel(le) du marketing, la récolte de consentement fait désormais partie de votre quotidien, que ce soit pour collecter des données à des fins de personnalisation, faire du ciblage publicitaire, augmenter votre base de contacts au travers d'opt-ins, etc. Comme nous l'avons vu, le RGPD encadre plus formellement les conditions à respecter pour que ce consentement soit considéré comme conforme au sens du RGPD.

Certains formats marketing encouragent plus que d'autres les opt-ins et la collecte de données conformes au RGPD. C'est le cas des formats interactifs de type quiz, jeux-concours, tests de personnalité ou encore sondages, que beaucoup de grandes marques et de grands médias utilisent. En plongeant totalement les visiteurs dans l'univers de l'annonceur, ces formats augmentent en effet de manière mécanique les taux de conversion observés.

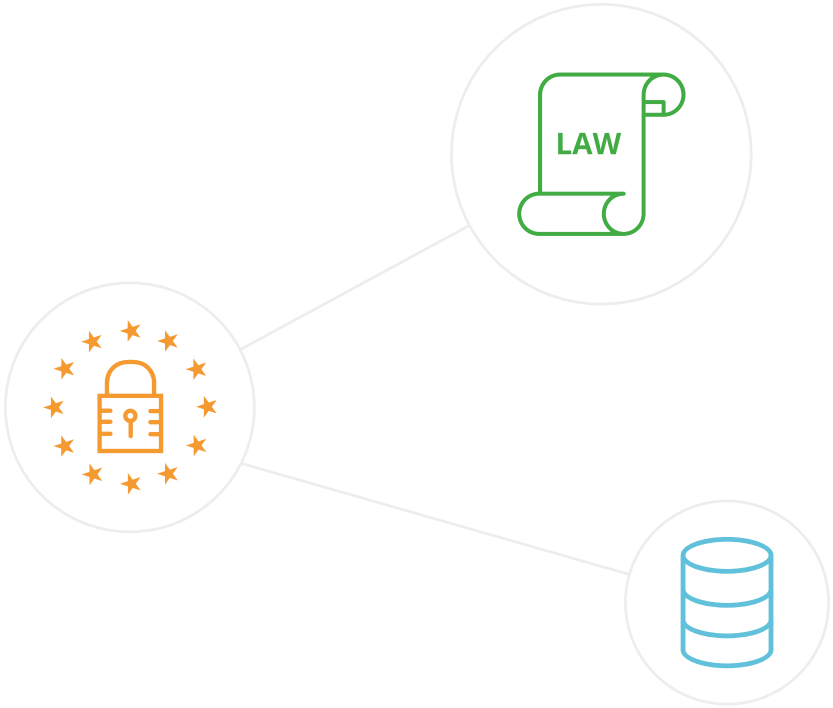
Mais ces formats ont un autre avantage dans un contexte post-RGPD: ils sont utilisés pour collecter des données « first-party » (c'est à dire obtenue directement auprès du *data subject*), via les formulaires qu'ils contiennent. Le RGPD renforce évidemment l'importance des données first-party par opposition aux données *second-party* et *third-party*, puisque les premières se fondent souvent sur la base légale du consentement.

Qualifio vous permet de créer ce type de contenus interactifs facilement et sans compétences techniques. La « boîte à outils RGPD » de Qualifio, ensemble de fonctionnalités dédiées au RGPD, vous permet d'assurer la conformité de toutes vos actions de marketing et de collecte dans Qualifio.

Conclusion

Par l'utilisation massive de données afin de segmenter et qualifier leurs audiences, les professionnels du marketing font face à de nombreux défis afin de **comprendre et respecter les règles du RGPD et de l'*e-Privacy***. Il est désormais plus que nécessaire de se mettre en conformité, sous peine de lourdes sanctions.

Nous l'avons vu dans cet e-book : que ce soit sur les réseaux sociaux ou votre propre site internet, le recueil de **consentement**, la responsabilité du **traitement des données à caractère personnel**, la sécurité et la rétention de ces mêmes données,... tout ceci est important afin d'engager les consommateurs et clients en toute légalité.



À propos des auteurs

Nathan Vanhelleputte est inscrit au Barreau de Bruxelles depuis février 2018.

Après deux années passées à travailler pour la société d'assurances AIG, il quitte l'entreprise américaine pour participer à la fondation d'un cabinet de consultance spécialisé dans les matières de la Compliance et du Regulatory.

C'est après cette expérience qu'il décide de rejoindre **Lex4u** pour y travailler notamment sur les matières de droit commercial, droit des contrats, droit de la protection des données à caractère personnel ainsi que le droit des nouvelles technologies.

Nathan est DPO certifié par la Solvay Brussels School.

Adeline Balza est passionnée par les nouvelles technologies ainsi que toutes les problématiques liées à la propriété intellectuelle et industrielle. C'est pourquoi, après avoir terminé son Master en Droit à l'Université Libre de Bruxelles en juin 2017, elle décide de poursuivre ses études en anglais à la Katholieke Universiteit Leuven afin de se spécialiser en Droit de la Propriété Intellectuelle et Droit des Technologies de l'Information et de la Communication.

Après avoir obtenu son Master Complémentaire en juillet 2018, Adeline rejoint Lex4u en octobre 2018 pour y pratiquer essentiellement le droit de la protection des données à caractère personnel et le droit des nouvelles technologies.

Mehdi Benallal est directeur marketing chez Qualifio, la plateforme leader dans le marketing interactif et la collecte de données. Il est membre du comité RGPD chez Qualifio et intervient régulièrement dans des conférences sur l'impact du RGPD sur les activités marketing des entreprises.

À propos de Qualifio

Qualifio est la plateforme de référence en Europe dans le marketing interactif et la collecte de données. Elle permet de créer et de publier facilement des contenus interactifs viraux (quiz, jeux-concours, enquêtes et plus de 50 autres formats innovants) sur tous les canaux digitaux.

Comment ça marche ?

Créez

Choisissez votre campagne interactive et customisez-la sans aucune intervention technique.

Publiez

En quelques clics, publiez votre campagne sur vos sites, apps, réseaux sociaux ou sur un mini-site dédié.

Collectez des données

Menez des campagnes 100% conformes au RGPD grâce à un ensemble de fonctionnalités dédiées.

Obtenez des résultats

Consultez et exportez les données collectées et les statistiques de vos campagnes en temps réel.

Segmentez & monétisez

Connectez Qualifio à vos outils marketing et data (CRM, DMP, e-mail, automatisation, SSO, Analytics, etc.).

Ce contenu vous a plu ?

INSCRIVEZ-VOUS À NOTRE NEWSLETTER

Plus d'infos sur Qualifio ?

CONTACTEZ-NOUS

www.qualifio.com