Leto

Conformité RGPD pour les équipes marketing & commerciales

Checklist

LETO. LEGAL

SOMMAIRE

LES POINTS CLÉS

Nous aborderons dans ce livre blanc tous les éléments que vous devez mettre en place pour vous assurer d'avoir une stratégie marketing et commerciale en conformité avec le RGPD pour développer votre activité en toute sérénité.

INTRODUCTION MARKETING, VENTE & RGPD

À l'ère du numérique, où les données personnelles sont devenues une ressource cruciale pour les entreprises, la conformité au Règlement Général sur la Protection des Données (RGPD) est plus qu'une exigence légale, c'est une pierre angulaire de la confiance et de l'intégrité. Les stratégies marketing et commerciales d'aujourd'hui s'appuient largement sur la collecte, l'analyse et l'utilisation de données, ce qui place les questions de conformité au RGPD au cœur de ces activités.

Pour les équipes commerciales et marketing, la conformité au RGPD n'est pas seulement une question de se conformer à la loi, elle est intrinsèquement liée à la capacité de construire des relations durables et de confiance avec les clients. Dans un contexte où les consommateurs sont de plus en plus conscients et exigeants en matière de protection de leurs données, ignorer le RGPD peut non seulement entraîner des sanctions légales, mais aussi nuire à la réputation et à la crédibilité d'une entreprise.

En effet, d'une part, un manquement au RGPD comme les envois non sollicités, l'absence de possibilité de se désabonner ou encore l'absence de réponse à un exercice droit vous exposent à une sanction de la part de la CNIL. Le RGPD prévoit des sanctions pouvant être très lourdes : jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial.

D'autres part, la protection des données personnelles, un sujet de préoccupation croissante pour les citoyens européens. Selon un sondage Eurobaromètre, 92% des Européens considèrent la protection des données personnelles comme un droit fondamental. Les entreprises qui prennent au sérieux la confidentialité et la sécurité des données gagnent en réputation et en confiance auprès de leurs clients et partenaires.

De plus, dans son rapport annuel, la CNIL déclare que plus d'un tiers de sanctions prononcées concerne un manquement à la sécurité des données ayant entraîné une fuite de données personnelles des individus. En plus du coût financier évident, c'est un coût réputationnel incalculable pour l'organisme visé par un tel incident et une rupture du lien de confiance avec vos clients et partenaires.

C'est pourquoi comprendre et intégrer le RGPD dans les stratégies de marketing et de vente est crucial. Cela implique une approche minutieuse de la collecte de données, un respect strict des droits des individus et une transparence absolue dans les processus de traitement des données.

Ce guide pratique a pour but d'éclairer les entreprises sur les meilleures pratiques de conformité au RGPD, spécifiquement dans le contexte des équipes commerciales et marketing, et de montrer comment ces pratiques peuvent se transformer en avantages compétitifs significatifs.

1 - LES BASES DE LA CONFORMITÉ RGPD

La conformité au Règlement Général sur la Protection des Données (RGPD) est cruciale pour les équipes commerciales et marketing. Néanmoins, avant de s'appliquer aux process sales & marketing, un certain nombre de règles plus génériques doivent être rappelées pour s'appliquer à l'ensemble de vos activités. Il s'agit principalement de principes fondamentaux concernant la protection des données personnelles.

Qu'est-ce que le RGPD ?

Le Règlement Général sur la Protection des Données (RGPD) est une réglementation de l'Union européenne en vigueur depuis mai 2018. Avant cette date, la loi Informatique et Liberté de 1978 en France réglementais déjà largement le sujet de la protection des données personnelles. Cette règlementation vise à renforcer et unifier la protection des données pour les individus au sein de l'Union européenne.

Le RGPD a deux objectifs principaux :

- Responsabiliser les entreprises sur la manière dont les entreprises collectent, stockent, traitent et sécurisent les données personnelles.
- Permettre à chaque individus d'exercer un certain nombre de droits sur leurs données personnelles comme s'opposer à l'utilisation de leurs données personnelles par une entreprise.

À qui s’adresse le RGPD ?

À tous les organismes

Le RGPD s'applique à tous les organismes, quelle que soit leur taille, et couvre toutes les activités professionnelles dans l'Union européenne. Il exclut uniquement les traitements de données personnelles réalisés à des fins strictement personnelles ou domestiques. Tous les types d'organismes, y compris les auto-entrepreneurs, les petites et grandes entreprises, les administrations, les ONG et les associations, sont concernés par cette réglementation.

De plus, le RGPD s'applique également en dehors des frontières de l'Europe, concernant les organismes établis dans l'UE qui opèrent en dehors de celle-ci, ainsi que les organismes hors UE traitant des données de personnes de l'UE.

À toutes les données personnelles

Le RGPD s'applique à toutes les données à caractère personnel, ce qui englobe une gamme étendue d'informations.

💡 Selon l'article 4 du RGPD, les données personnelles comprennent toute information se rapportant à une personne physique identifiable, que cette identification soit directe (comme le nom et prénom) ou indirecte (par exemple, le numéro de sécurité sociale, l'adresse e-mail, ou même des enregistrements de conversations).

Sont donc exclues de cette définition toutes les données se rapportant à une personne morale (entreprise, organisme privé ou public, État etc.).

Cette définition englobe donc pratiquement toute information qui peut être reliée à une personne, élargissant considérablement le champ d'application du RGPD. Cela signifie que presque toutes les données collectées, traitées, ou stockées par un organisme dans un contexte professionnel doivent être gérées conformément aux principes et exigences du RGPD, garantissant ainsi un niveau élevé de protection et de confidentialité des données personnelles.

Quelles sont les règles de bases du RGPD ?

Le RGPD se fonde sur quelques grands principes fondamentaux de la protection des données personnelles qui doivent en permanence guider vos opérations :

- **Licéité, loyauté et transparence** (article 5 RGPD) : la licéité signifie que la collecte de données personnelles doit être légale (6 cas sont énumérés dans l'article 6 RGPD), par exemple obtenir le consentement des personnes. La loyauté interdit la collecte ou l'utilisation trompeuse de données personnelles et la transparence nécessite d'informer clairement les personnes sur l'utilisation de leurs données et leurs droits y afférents.

- **Limitation des finalités** : Toute opération, ou traitement de données personnelles, doit être uniquement guidée par une finalité, c'est-à-dire une raison qui limite l'utilisation de ces données à un but donné. La finalité doit être spécifique à un traitement, explicite et légitime.

- **Minimisation des données personnelles** : seules les données nécessaires pour les finalités du traitement doivent être collectées. En pratique, ce principe incite les entreprises à se demander si les données qu'elles collectent sont réellement nécessaires à leur activité. Si ce n'est pas le cas, ces données doivent être supprimées, anonymisées ou leur collecte doit être limitée à ce qui est essentiel.

- **Limitation de la durée de conservation des données personnelles** : Le principe de limitation de la conservation des données du RGPD stipule que les entreprises ne peuvent pas garder indéfiniment les données personnelles. Une durée de conservation spécifique doit être établie avant la collecte des données. Cette durée peut être définie par un délai précis (par exemple, 6 mois ou 3 ans) ou par un événement spécifique (comme la fin d'un contrat ou le désabonnement d'une newsletter). Une fois cette période expirée, l'entreprise doit soit supprimer les données personnelles, soit les anonymiser pour qu'elles ne soient plus associées à une personne identifiable, et ainsi, ne relèvent plus du RGPD.

- **Sécurité des données personnelles** : le traitement de données personnelles implique l'adoption de mesures de sécurité appropriées. Les entreprises doivent maintenir la confidentialité des données personnelles et prévenir toute forme de violation (comme la modification, la divulgation, la perte, le vol, ou la destruction intentionnelle ou accidentelle de ces données). Selon l'article 32 du RGPD, ces mesures de sécurité peuvent être de nature organisationnelle, technique ou physique, et doivent être efficaces pour minimiser les risques de violation de données.

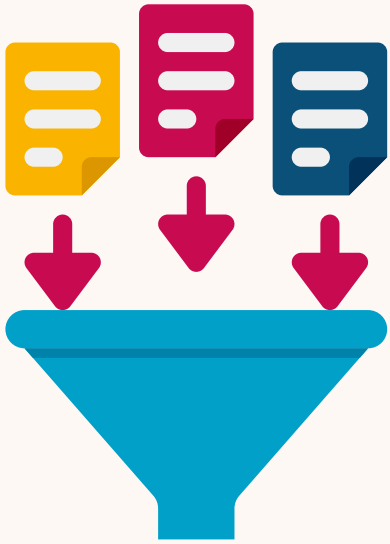
Vous l'aurez compris, le RGPD impacte significativement les pratiques de marketing et de vente, exigeant une révision des méthodes de collecte, de stockage et d'utilisation des données clients. Il oblige les entreprises à obtenir un consentement explicite pour le traitement des données, à informer clairement les individus sur l'utilisation de leurs données, et à garantir la sécurité des données traitées.

2 - Marketing et commercial : checklist RGPD

Le RGPD n’est pas qu’une réglementation théorique. Le règlement a des implications très concrètes au quotidien. Les entreprises doivent être particulièrement attentives à la manière dont sont traitées les données personnelles des prospects et des clients en fonction de son statut de client ou de prospect, de particulier ou de professionnel, en fonction du canal de communication et surtout en fonction de la finalité du traitement.

Conformité RGPD dès de la collecte d’informations

L’un des premiers chantiers est le site web qui constitue une porte d’entrée pour le développement commercial et la stratégie de marketing digitale. Par ce canal, un certain nombre de données personnelles sont collectées. Encore faut-il avoir les bonnes pratiques.



Des formulaires RGPD friendly

La plupart des données personnelles sont collectées via des formulaires de collectes. Vous pouvez ainsi collecter des données personnelles pour l'inscription à un webinair, le téléchargement d'un livre blanc, ou tout simplement pour la création d'un compte client ou utilisateur de la plateforme. Bref, tout autant de finalité qu'il existe de cas de figure possible. En toute hypothèses, il convient d'avoir les bons réflexes.

Ne colleter que les données nécessaires

Cette règle est aussi appelée "principe de minimisation des données". Il signifie que l'organisme ne collecte que les informations indispensables à son activité. Autrement dit, plus vous limitez la collecte de données, plus vous vous rapprochez de la conformité. Cette règle implique de se demander si les données qu'elles collectent sont réellement nécessaires à la finalité poursuivie. Si ce n'est pas le cas, ces informations ne doivent être demandées.

Par exemple, lorsqu'un utilisateur souhaite télécharger un livre blanc pour développer votre base de lead à rappeler, vous n'avez besoin que de son identité, ses coordonnées et peut-être même son secteur d'activité. Il n'est pas nécessaire de lui demander sa date de naissance.

Recueillir le consentement préalable en B2C

Le consentement est obligatoire dans tous les cas de figure : formulaire de contact, formulaire de téléchargement, formulaire d'inscription, formulaire de demande de rendez-vous etc. Ce consentement doit prendre une forme précise : libre, spécifique, éclairé et univoque. Pour se faire, le consentement doit être récoltée par un "opt-in", c'est-à-dire un accord préalable par un "oui" et pas un "non je m'y oppose". Une cache non cochée doit être mise à disposition.

Par exemple : " [ ] J'accepte que mes informations soient utilisées pour de la prospection commerciale/ pour recevoir des offres de la société X"

Ce consentement doit être récolté préalablement à tout future communication.

⚠ Attention le consentement doit être récolté par une finalité. Si ces données vont être réutilisée pour d'autres finalités, il convient de dédié une case pour chaque finalité.

L’information systématique des personnes

L’information des personnes à propos du traitement est obligatoire au moment de la collecte des données personnelles (B2C et B2B) et préalablement à toute communication future. Les personnes doivent ainsi être informées des éléments suivants :

- l’identité du responsable de traitement (votre entreprise),
- la finalité du traitement (par exemple : pour l’envoie de newsletter),
- la base légale du traitement (par exemple : le consentement de la personne concernée),
- les personnes ayant accès à ces données, c'est-à-dire votre entreprise et tout autre outil utilisé pour le traitement de ces données comme un CRM (par exemple Hubspot) et/ou un outil d’emailling (par exemple Mailchimp).
- La manière dont les personnes peuvent exercer leurs droits sur les données (par exemple se désinscrire),
- La durée de conservation de ces données.

En pratique ces informations peuvent être centralisées dans un document auquel le formulaire fait référence, comme votre Politique de confidentialité ou vos conditions générales de ventes (CGV) ou conditions générales d’utilisation (CGU). La Politique de confidentialité est la meilleure pratique car elle permet d’avoir une page dédiée aux détails des traitements de données personnelles.

Permettre les exercices des droits

Il est primordial de donner accès publiquement à votre politique de confidentialité facilement depuis votre page d'accueil et sur tous les formulaires de collecte de données personnelles. Ce document doit contenir un certain nombre d'éléments obligatoires (article 13 du RGPD) relatifs aux traitements de leurs données personnelles par finalité et à la sécurité des données. Cela peut inclure des mesures techniques (comme l'anonymisation, la pseudonymisation) et des mesures organisationnelles (comme la sensibilisation du personnel).

Surtout, les personnes doivent avoir la possibilité d'exercer leurs droits facilement. Il est crucial d'informer les utilisateurs de leurs droits en vertu du RGPD, notamment leurs droits d'accéder à leurs données (article 15 RGPD), de les corriger (article 16 RGPD), de demander leur suppression (article 17 du RGPD), de s'opposer à leur traitement pour une finalité précise (article 21 du RGPD) et de demander leur portabilité (article 20 du RGPD). Vous devez également informer les internautes de leur possibilité d'introduire une réclamation auprès de la CNIL.

💡 Conseil pratique, équipez-vous d'un Privacy Portail pour permettre de rassembler tous ces éléments dans un seul endroit accessible depuis votre page d'accueil :

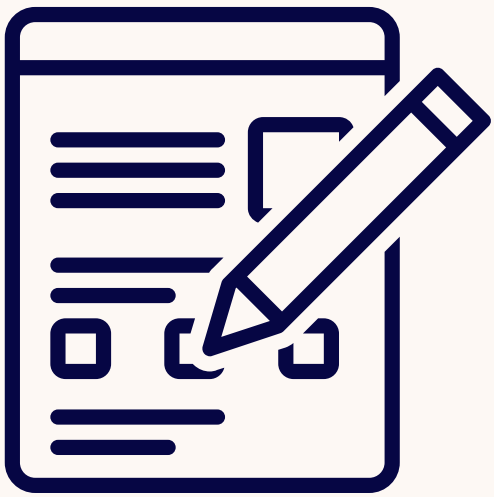
- Politique de confidentialité
- Portail pour exercer ces droits
- Politique de sécurité

Le logiciel RGPD Leto propose un Privacy Portail permettant de communiquer de manière transparente sur votre démarche en matière de protection des données personnelles et votre conformité au RGPD avec l'ensemble de votre documentation accessible en un clic.

💡 Exemple de mentions légales pour un formulaire de collecte conforme au RGPD :

"[ ] J'accepte que mes informations soient utilisées pour de la prospection commerciale/ pour recevoir les dernières actualités et offres spéciales par e-mail / pour resté informé de nos prochains webinar / pour la création d'un compte utilisateur etc.[Nom de votre entreprise] traite les données recueillies pour [finalités du traitement].

Pour en savoir plus sur la gestion de vos données personnelles et pour exercer vos droits, reportez-vous à la politique de confidentialité [ajouter le lien]"



Cookies et traceurs

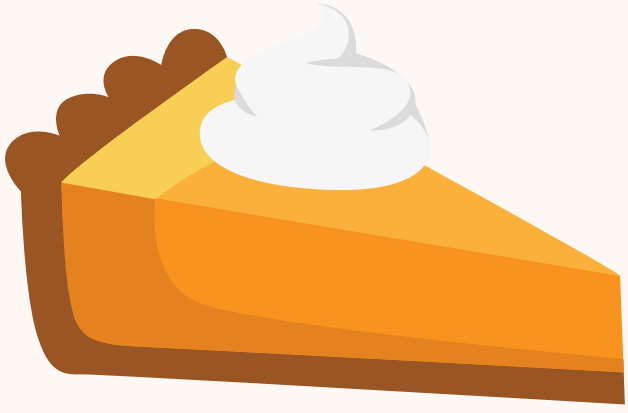
Les cookies ou traceurs permettent de collecter un grand nombre de données personnelles sur la personne qui navigue sur votre site web comme son adresse IP, son historique de navigation, ses préférences etc. Certains cookies sont exempts de tout consentement comme ceux indispensables au bon fonctionnement du site web (par exemple le cookie qui permet de sauvegarder la langue choisie par l'utilisateur). Pour le reste, les cookies et autres types de traceurs ne peuvent être déposés qu'en échange du consentement de la personne par un petit bandeau de cookie préalablement à la navigation.

Pour être conforme, votre outil de cookies doit :

- Utiliser un système de cases à cocher ou de sliders (désactivé par défaut) pour permettre à l'utilisateur de valider ou non son consentement
- L'utilisateur doit pouvoir préciser son consentement pour chaque cookie déposé par le site web ou l'application.
- La personne doit être informée des cookies qui vont être déposée sur son navigateur et doit pouvoir changer d'avis.

Cela n’empêche pas, cependant, de proposer à l’utilisateur un bouton unique pour consentir ou refuser le consentement globalement. Typiquement “Tout accepter” et “Tout refuser”. Dans ce cas de figure, il est important en revanche que les 2 boutons aient le même rendu visuel. A garder également en tête : si l’internaute ne refuse ni n’accepte explicitement son consentement (par exemple en fermant une pop-up), cela doit être considéré comme un refus de consentement.

Il est également recommandé de laisser apparent sur l’écran une petite icône qui permette à l’utilisateur de revenir sur la pop-up du choix de consentement. Aujourd’hui beaucoup d’outils propose ce service comme par exemple Tarte au citron.



Le cas des courtiers de Données (Data Brokers)

Les courtiers de données, ou Data Brokers, collectent des informations sur les individus auprès de diverses sources et les vendent à des entreprises pour leurs efforts de marketing. Le RGPD impose des obligations strictes aux entreprises qui utilisent ces services. Vous devez être très attentif lors de l'achat de bases de données et vérifier les éléments suivants :

- Informer les personnes concernées dès le premier contact ou, au plus tard, dans un mois, sauf si elles ont déjà reçu les informations nécessaires. Cette information doit inclure la source des données, c'est-à-dire le nom de la société qui a vendu le fichier client.

- Vérifier que chaque personne dans cette liste ait donné son consentement éclairé pour utiliser leurs données à des fins de prospection commerciale électronique. Assurez vous que l'entreprise est en mesure de prouver le consentement des personnes avant l'achat ou après l'achat vous devez collecter le consentement des personnes avant de procéder à la prospection électronique.

Le cas des données librement accessibles sur internet ou le scraping de données

Soyez vigilant avec les données que vous collectez sur internet librement accessibles. Ces données personnelles sont également protégées par le RGPD. Le fait que ces données soient publiquement accessibles ne vous exempte pas d'obligations en vertu du RGPD.

En effet, de nombreux outils permettent de faire du "scraping" de données sur internet. Ici les mêmes règles s'appliquent :

Cas n°1 : dans une relation B2C, vous ne pouvez pas utiliser ces données si les personnes n'ont pas préalablement donné leur consentement.

Cas n°2 : dans une relation B2B, vous pouvez les réutiliser si 3 conditions sont remplies :

- Le démarchage commercial est en lien directe avec la profession de la personne,
- Lors de la 1ère communication, vous informez la personne du traitement de ses données (au moins la finalité de la communication et un lien vers votre politique de confidentialité).
- Dans toutes les communications, veillez à permettre au destinataire de disparaitre de votre liste de diffusion et ainsi lui permettre de s'opposer au traitement.

Conformité RGPD de vos communications marketing et commerciales

La mise en oeuvre opérationnelle de votre conformité RGPD s'exécute au travers de deux grandes étapes majeures que sont :

- Le bon choix et paramétrage de vos outils,
- La bonne rédaction des mentions légales RGPD lors de vos communications marketing ou commerciales.

Choisir des outils RGPD friendly

Le choix d'un outil de communication marketing ou d'un CRM est indispensable car votre organisme est responsable de la capacité de votre sous-traitant à assurer la protection des données personnelles qui transitent par cet outil.

💡 Selon l'article 4 du RGPD, le responsable de traitement est la personne morale qui détermine la finalité et les moyens du traitement de la donnée personnelle. Le sous-traitant est la personne ou l'organisme (souvent un prestataire de service) qui traite des données à caractère personnel pour le compte et sur les instructions du responsable de traitement.

Par exemple : une entreprise A offrant une service d'envoi de newsletters (par exemple Mailjet) utilise le fichier clients mis à sa disposition par l'entreprise B (votre entreprise). L'entreprise A est le sous-traitant de l'entreprise B, responsable de traitement.

Dans notre cas de figure, l'outil choisi pour la communication marketing est votre sous-traitant et, puisque les données de vos prospects et clients sont automatiquement transférées dans cet outil, le sous-traitant doit lui-même être conforme RGPD.

Comment savoir si mon sous-traitant (outil/prestataire) est conforme RGPD ?

Vous devez vous référer au contrat signé avec votre prestataire ou son DPA (Data processing agreement) et vérifier qu'il s'engage à :

- Indiquer clairement comment sont traitées les données transférées : prestation effectuée, stockage, hébergement, nature du traitement, finalité, durée de conservation, transfert des données vers un autre sous-traitant.
- Surtout qu'elles sont les mesures de sécurité mises en oeuvre pour assurer leur confidentialité.
- Enfin, tout traitement opéré pour votre compte doit être sur vos instruction et cette mention doit apparaitre dans le contrat.

Il est devenu courant d'auditer ses sous-traitants avant tout transfert de données, par exemple à l'aide d'un questionnaire RGPD voir de négocier le DPA afin que le sous-traitant assure un haut niveau de protection des données que vous lui transférez.

Si vous vous interrogez sur un outil, rendez-vous sur notre page dédiée à l'analyse de la conformité de chaque outil.

Ajouter les bonnes mentions RGPD

L’envoi de campagnes marketing est aujourd’hui assez incontournable pour communiquer sur votre produit ou service qu’il s’agisse de l’arrivée de nouvelle features, de l’évolution de vos services, de l’actualité de votre entreprise ou du secteur ou enfin pour des offres promotionnelles. L’ensemble de ces règles sont également applicables à vos actions de prospections commerciales (inbound et outbound).

Cette partie est la plus importante car elle représente la partie visible de l’iceberg : le recueil du consentement, l’information des personnes et la possibilité d’exercer ses droits. Voyons ensemble comment naviguer dans ces règles selon les segments B2B (Business-to-Business) et B2C (Business-to-Consumer). L'approche diffère en raison de la nature des données traitées et des relations établies mais certaines règles sont communes.

Les règles RGPD en B2C

Comme vu plus haut, le consentement préalable est obligatoire préalablement à toute communication (par exemple avant l'envoie d'email marketing ou newsletter). Ce consentement doit être recueilli à l'aide d'un opt-in. Une personne qui consent à la collecte d'information de certaines de ces données via un formulaire par exemple n'est pas suffisant pour que vous la placiez dans votre liste de diffusion. Cette personne doit spécifiquement avoir consenti à recevoir ce type spécifique de communication. Pour vous assurer de la conformité de l'envoi de newsletter (par exemple), mettez en place un système de double opt-in :

- Une case à cocher ;
- Demander au destinataire de confirmer son consentement via l'adresse de messagerie communiquée.

⚠ **Assurez-vous de pouvoir garder une trace de ce consentement dans un outil.**

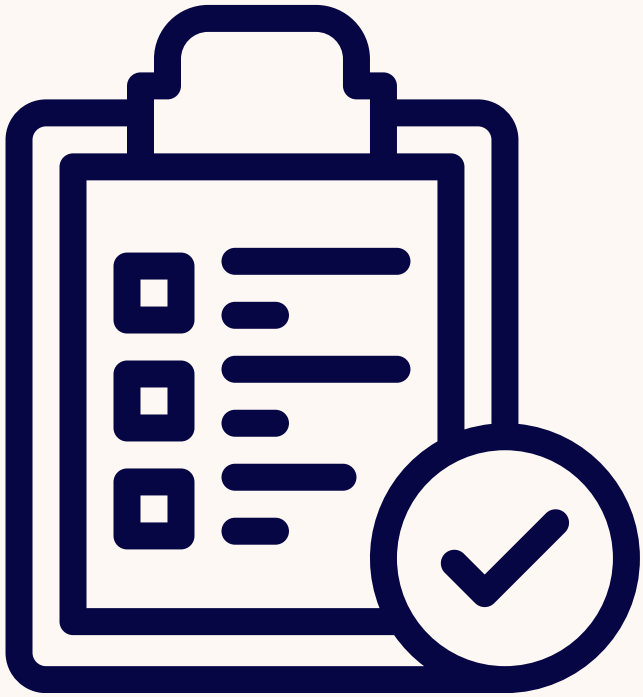
Ces règles sont applicables dans tous les cas de figure : démarchage commercial, communication marketing etc. Le destinataire doit avoir consenti préalablement de manière claire, spécifique et univoque.

Par exemple : "[ ] J'accepte que mes informations soient utilisées pour de la prospection commerciale. Pour en savoir plus sur la gestion de vos données, rendez-vous sur notre politique de confidentialité [ajouter le lien]"

De plus, dans chacune de vos communications, vous devez offrir des options faciles et gratuite pour :

- Informer votre destinataire de la manière dont sont traitées leurs données personnelles. Le cas échéant, juste par un lien vers vers votre politique de confidentialité.
- Permettre à vos destinataire de facilement et rapidement, retirer leur consentement en s'opposant aux traitements de leurs données (ou de désincrire de la newsletter).

Par exemple : "Pour en savoir plus sur la gestion de vos données, rendez-vous sur notre politique de confidentialité [ajouter le lien].
Plus envie de recevoir nos e-mails ? Cliquez ici 😢 [ajouter le lien] "



Les règles RGPD en B2B

Là où dans une relation B2C, le consentement préalable est obligatoire, la CNIL est plus indulgente dans une relation B2B. Dans un tel cas, vous pouvez vous appuyer sur l'intérêt légitime de votre organisme (base légale du traitement).

💡 Pour rappel, il y a toujours des données personnelles dans une relation B2B telles que les noms et les adresses e-mail des employés. Si vous envoyez un email à une adresse email générique type "contact@entreprise.com", aucune donnée personnelle n'est en jeux ainsi le RGPD ne s'applique pas.

⚠ Attention, il est possible de prospecter en B2B sans consentement préalable uniquement lorsque l'emailing est en rapport avec la profession de la personne démarchée. Dans le cas contraire, le consentement est requis.

Alors si le consentement n'est pas obligatoire, quelles sont les mentions RGPD qui doivent être présentes dans toutes communications marketing ou de prospection commerciales B2B ?

- L'information claires sur la manière dont leurs données sont utilisées et comment ils peuvent exercer leurs droits selon le RGPD.
- La possibilité de s'opposer à ce traitement simplement et gratuitement. Il est essentiel de fournir une option de désinscription claire et de ne pas collecter plus de données que nécessaire.

Exemple n°1 : "Vos données personnelles informations sont utilisées pour de la prospection commerciale. Cliquez ici si vous ne souhaitez plus que vos informations soient utilisées pour recevoir des offres de la société X par courrier électronique"

Exemple n°2 : "Pour en savoir plus sur la gestion de vos données personnelles et pour exercer vos droits, reportez-vous à la politique de confidentialité [ajouter le lien] "

Les règles RGPD communes en B2C et B2B

Pour résumer, dans un cas comme dans l'autre, votre organisme doit faire preuve d'une transparence complète et respecter les droits des personnes concernées. Ces principes sont essentiels pour maintenir la confiance des clients et se conformer à la réglementation.

Pour rappel, deux éléments sont essentiels :

1. L'information complète des personnes. Un lien vers la politique de confidentialité détaillée est acceptée.
2. Le droit d'opposition à ce traitement (ou le désabonnement) doit être facile et gratuit. Un lien vers une page de désincription ou un portail d'exercice des droits est une bonne pratique.

💡Pour rappel, vous avez 30 jours pour donner suite à toute demande d'exercice de droit.

- Pour les demandes de suppression de données de santé le délai est de 8 jours.
- Pour toutes autres demandes, le délai est de 30 jours.
- En cas de difficulté particulière (par exemple pour identifier le demandeur), ce délai peut aller jusqu'à 3 mois.

Au delà de ce délai, la personne concernée a la possibilité de signaler un abus directement auprès de la CNIL ce qui déclenche souvent un contrôle de sa part.

3 - Assurer sa conformité RGPD dans le temps

La conformité RGPD a plusieurs versants : la partie émergée de l'iceberg et opérationnelle qui tient à la mise en place des bonnes mentions légales dans les formulaires et communications, la récolte du consentement, la publication d'une politique de confidentialité etc. Mais il existe une grande partie de la conformité qui réside dans la construction de documents internes qui sont absolument nécessaires en cas de contrôles des autorités ou d'audit. Ces documents s'accompagnent également de mises en oeuvre de mesures concrètes en interne.

Construire son registre des traitements

Le registre de traitement est votre boussole RGPD (article 30 RGPD). C'est un document obligatoire pour chaque entreprise et qui a pour objet de recenser tout vos traitements de données personnelles. C'est le document de référence permettant de démontrer votre conformité auprès des autorités de contrôles.

Pour chaque traitement, vous devez renseigner un certain nombre d'éléments. En ce qui concerne le marketing et la prospection commerciale, voici à quoi vos traitements pourraient ressembler :

- Type de données collectées : nom, prénom, adresse e-mail, profession etc.
- Personnes concernées : prospects ou clients.
- Bases légales : consentement (B2C) ou intérêt légitime (B2B).

💡 Selon l'article 4 du RGPD, la base légale permet à l'organisme de s'assurer qu'il traite légalement des données personnelles. L'article 6 du RGPD énumère 6 cas dont 4 intéressent les entreprises :

- **L'obligation légale** : si une loi oblige l'organisme à traiter des données personnelles.
- **Le contrat** : si l'exécution d'un contrat (par exemple le contrat client) oblige l'organisme à traiter des données personnelles.
- **Le consentement** : dans les hypothèses vues précédemment, certains traitements de données requièrent un consentement obligatoire.
- **L'intérêt légitime** : en l'absence des 3 cas susmentionnés, l'entreprise peut fonder le traitement de données personnelles sur son intérêt légitime. Tel est le cas de la prospection commerciales B2B.

- Finalités : par exemple, développer sa base de données prospects, maximiser le trafic sur un site web, construire et maintenir une communauté autour de la marque, augmenter le chiffre d'affaires de l'entreprise, fidéliser les clients etc.
- Responsabilité : pour toutes les activités marketing et commerciales, l'organisme est entière responsable.
- Durée de conservation : par exemple la CNIL recommande une durée de conservation de 3 ans après le dernier contact avec un prospect ou jusqu'à désincription.
- Sous-traitants : par exemple les outils tels que Mailjet, Hubspot, Salesforces, Mailchimp, Brevo.

Faire le ménage dans ses données personnelles

Conformément à ce que vous avez déclaré dans le registre concernant les durées de conservation des données, supprimez ou anonymisez les données lorsqu'elles ne sont plus pertinentes. Par exemple, la CNIL recommande de supprimer les données de prospects 3 ans maximum après le dernier contact. En ce qui concerne les données de cookies, la CNIL recommande une durée maximum de 25 mois à compter de la collecte.

Il est donc recommandé de repasser régulièrement sur votre CRM pour éliminer les données obsolètes. Cette pratique vous permet également de mettre régulièrement à jour votre base de données contact.

⚠ **Surtout, retirez de votre liste de diffusion les personnes pour lesquelles vous n'avez pas la preuve de leur consentement, ceux qui ont retirer leurs consentement ou qui s'y sont opposés (valable en B2C comme en B2B). En cas de de plainte, la sanction pourrait être lourde.**

Sécuriser les données personnelles

Le RGPD impose également à toutes les organisations d'adopter des mesures de sécurité qui permettent d'assurer la protection des données personnelles et prévenir tout accès, fuite, perte ou destruction non autorisée. Le RGPD parle de "violation de données personnelles". Pour cela, votre organisme a donc pour devoir de mettre en place des mesures de sécurité (article 32 RGPD).

💡 Selon l'article 4 du RGPD, une violation des données à caractère personnel correspond à une violation de leur sécurité entraînant, de manière intentionnelle ou non, la destruction, la perte, la divulgation ou l'accès non autorisé.
Il s'agit d'un incident de sécurité qui peut aussi bien provenir d'une malveillance externe (par exemple un piratage conduisant au transfert des données) ou d'un accident interne (par exemple, incident informatique conduit à la suppression des données personnelles).

Quelques exemples de mesures de sécurité :

- Utilisation de mots de passe robustes et de l'authentification à deux facteurs.
- Sécurisation des locaux physiques de l'entreprise (vidéosurveillance, les systèmes d'alarme et les contrôles d'accès biométriques).
- Sensibilisation et formation des employés sur les enjeux du RGPD et de la sécurité des données.
- Gestion stricte des droits d'accès aux bases de données.
- Utilisation de pare-feux, de systèmes de détection et de prévention des intrusions, ainsi que du chiffrement des données.
- Mise en place de sauvegardes régulières et stockage sécurisé hors site.
- Mise à jour régulière des logiciels, systèmes d'exploitation et applications.
- Sécurisation des dispositifs connectés (endpoints) pour éviter les cyberattaques.
- Mise en place de politiques de sécurité claires et leur suivi par tous les employés, pouvant être intégrées dans la Politique de confidentialité de l'entreprise.
- Choix un logiciel RGPD permettant de maitriser la confidentialité et la sécurité des données personnelles.

Conclusion

En résumé, naviguer dans le paysage complexe du RGPD peut sembler intimidant, mais c'est une démarche cruciale pour toute entreprise souhaitant renforcer la confiance et la fidélité de ses clients. La conformité au RGPD ne se limite pas au respect de la loi, elle offre également l'opportunité de bâtir une relation de confiance et de transparence avec les clients.

C'est dans cette perspective que Leto, notre logiciel SaaS, a construit une solution qui permet d’automatiser une grande partie de la mise en conformité et de gagner un temps précieux.

FAITES CONFIANCE À LETO

Comment mettre en œuvre le RGPD dans une entreprise de manière efficace ? Comment transformer cette contrainte réglementaire en opportunité de développement de son activité ?

C'est en partant de ces enjeux rencontrés dans leurs expériences entrepreneuriales que Benjamin et Édouard ont créé Leto.

Leto est une solution Saas dont l'ambition est d'automatiser la mise en conformité au RGPD et d'en faire une réalité opérationnelle au quotidien dans l'entreprise.

POWDER

"L'équipe Leto nous a accompagné à chaque étape, nous permettant de gagner un temps précieux et de rassurer nos clients et partenaires quant à notre engagement en matière de protection des données personnelles de nos utilisateurs."
Kevin Cathaly, CTO de Powder

QOMON

"Nous sommes très satisfaits de la solution. Elle nous permet de répondre rapidement aux questions de nos prestataires sur le RGPD mais aussi les "privacy laws" en général qui voient le jour partout dans le monde. Les vrais plus avec Leto : la connexion automatique et le fait de pouvoir engager les équipes en interne autour de la protection des données personnelles de nos utilisateurs ".
Florent Barre, CEO chez Qomon

👉 Retrouvez tous nos témoignages Clients

LETO VOUS PERMET DE

Gagner du temps au quotidien

Leto réalise et maintient automatiquement l'inventaire des types de données personnelles traitées par l'organisation et toute la documentation de conformité.

Raccourcir votre cycle de vente

Leto aide vos équipes (commerciale, compliance, etc.) à répondre aux audits et questionnaires conformité de vos prospects

Réduire votre risque réputationnel

Leto aide vos équipes (commerciale, compliance, etc.) à répondre aux audits et questionnaires conformité de vos prospects

Améliorer la maturité des équipes

Leto sensibilise l'ensemble vos collaborateurs à la protection des données personnelles grâce une technologie unique de microlearning ultra-personnalisé.

ENVIE D'EN SAVOIR DAVANTAGE ?

N'HÉSITEZ PAS À NOUS CONTACTER.

NOTRE E-MAIL :
contact@leto.legal

NOTRE SITE WEB :
leto.legal

NOTRE NEWSLETTER :
leto.legal/newsletter-rgpd

NOTRE CHAINE YOUTUBE :
youtube.com/@letolegal

NOS LIVRES BLANCS :
leto.legal/livre-blanc/rgpd