Leto

ECOMMERCE ET RGPD : QUELS ENJEUX ?

NOS CONSEILS

LETO. LEGAL

SOMMAIRE

LES POINTS CLÉS

En 2022, le secteur du e-commerce a encore progressé de +10% et 14 000 sites marchands ont été créés sur un an (chiffres de la FEVAD).

Cet engouement ne doit pas faire oublier que la création et le fonctionnement d'une boutique en ligne sont encadrés par la loi, notamment en ce qui concerne la protection des données personnelles.

En effet, comme toute entreprise, un site e-commerce doit obligatoirement être conforme au RGPD au regard de la collecte des données personnelles et des droits des internautes.

- Comment mettre votre boutique en ligne en conformité avec le RGPD ?
- Quelles sont les actions essentielles à mettre en place ?

E-COMMERCE: LES 5 ETAPES CLES

Listez les données personnelles que vous collectez

Quelles sont les catégories de données personnelles que vous collectez ?

Les données personnelles sont définies à l'article 4 du RGPD comme toutes les informations se rapportant à une personne physique identifiée ou identifiable :

- directement : nom et prénom
- ou indirectement : coordonnées bancaires, adresse e-mail, adresse de livraison, enregistrement des conversations, préférences d'achat etc.

Faites la liste de toutes les informations que vous collectez directement ou indirectement lorsque les personnes remplissent des formulaires, créent leur compte, discutent avec un chatbot ou encore passent leurs commandes.

Si vous utilisez des outils telles que Google Analytics afin de récolter des informations sur le comportement de vos utilisateurs sur le site, n'oubliez pas qu'il s'agit de données personnelles également.
Pour l'ensemble des outils que vous utilisez (Shopify, Prestashop, Magento etc) la plateforme de Leto est capable de lister pour vous les données personnelles que vous collectez via cet outil.

Leto

Collectez-vous des données sensibles ?

Identifiez la nature des données personnelles que vous collectez. Le RGPD accorde une protection renforcée à certaines catégories de données. C'est le cas des données sensibles, des données relatives aux infractions pénales et infractions et des données perçues comme sensibles.

- Données sensibles (article 9 RGPD) : informations relatives à l'origine raciale ou ethnique, aux opinions politiques, aux convictions religieuses ou philosophiques, à l'appartenance syndicale, à la vie sexuelle ou orientation sexuelle, aux données génétiques et biométriques et données de santé.

Par exemple, l'achat d'un livre religieux peut potentiellement constituer une information sur les convictions religieuses de son acheteur. Mais pas d'inquiétude, dès lors que vous n'utilisez pas ces données pour ce qu'elles contiennent de sensible, c'est ok .

Leto

- Données relatives aux infractions pénales et infractions (article 10 RGPD) sont interdites de tout traitement par une entreprise.
- Données perçues comme sensibles : c'est une catégorie de données dont le périmètre est défini par la CNIL. Il ne s'agit pas de données sensibles listées à l'article 9 RGPD mais de données à qui on accorde une protection équivalente. Il s'agit des données bancaires et des données de géolocalisation.

Ces données, si vous les collectez, méritent une attention particulière car par principe vous ne pouvez les collecter et les utiliser que sous certaines conditions :

1. Vous devez impérativement être en mesure de prouver que la personne a explicitement donné son consentement.
2. De plus, vous devez bien sécuriser ces données. Étant donné qu'une fuite de ces données risque de porter atteinte à la vie privée des personnes, vous devez vous assurez de réduire le risque par tous moyens. Rendez-vous à l'étape 5 concernant la sécurisation des données ☺.

Ne collectez que les données nécessaires à votre activité

Le RGPD impose de ne collecter que les données qui sont strictement nécessaires à votre activité : c'est le principe de minimisation de la donnée. Ce principe signifie que la meilleure manière de protéger les données c'est encore de ne pas en collecter !

Comment faire le tri ? Comment choisir les données dont on a besoin et celle dont on peut se séparer ? Demandez-vous **quelles sont les données qui sont nécessaires à l'objectif poursuivi**.

Ne vous embarrassez pas de données personnelles que vous n'utilisez pas car si vous ne justifiez pas leur collecte par la poursuite d'un objectif précis, vous vous mettez dans une situation de risque au regard du RGPD.

Par exemple, si un site e-commerce vend des voyages, le e-commerçant aura besoin des données bancaires mais il n'est pas pertinent de demander le numéro de la carte de sécurité sociale.

⚠ Mettez en œuvre ce principe "By Design", c'est à dire dès la collecte des données. C'est un des principes fondateurs du RGPD : la Privacy By Design.

Au lieu de nettoyer vos données, ne collectez que les informations nécessaires dès le début. Concrètement : ne demandez à vos clients que ce qui est utile à votre activité et ne vous chargez pas davantage.

Leto

Auditez vos outils et vos sous-traitants

Pour rappel, 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 (article 4 RGPD).

Le responsable de traitement est la personne qui détermine la finalité et les moyens du traitement de la donnée personnelle.

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

Dans notre cas, vos sous-traitants peuvent être Shopify, Magento, Prestashop, Stripe, Paypal, Qonto, Salesforce, Hubspot.

Dès lors que vous faites appel à leurs services, vous transférez des données personnelles à ces entreprises.

Elles doivent alors être conformes et assurer une protection des données suffisantes.

Pour vous assurer que les pratiques des sous-traitants respectent les obligations RGPD, vérifiez les contrats que vous avez avec eux. En effet, les contrats doivent être conformes aux dispositions de l'article 28 du RGPD relatif aux sous-traitants.

L'élément le plus important à vérifier est l'immatriculation du sous-traitant, c'est-à-dire sa nationalité : l'entreprise est elle européenne, américaine, canadienne ?

Selon le pays d'origine de l'outil, celui-ci est soumis à une réglementation différente au point de vue de la protection des données personnelles. Il faut alors s'assurer que le droit assure une protection équivalente à celui du RGPD.

Par exemple, le droit US ne permet pas d'assurer une protection équivalente à celle du RGPD et ainsi par principe, l'utilisation d'outil américain est interdite sauf à ce que le contrat avec le sous-traitant prévoit des garanties supplémentaires.

Leto

Construisez votre registre de traitements de données personnelles

Le RGPD impose de faire la liste de **tous les traitements de données,** c'est-à-dire de ce que vous en faites : leurs collectes, leurs sauvegardes, leurs utilisations (pour une campagne marketing, une prospection commerciale, la gestion des commandes), pour quels objectifs, pendant combien de temps, comment sont elles sécurisées et à qui y a accès.

Leto

Le responsable de traitement est tenu d'alimenter un **registre listant les traitements de données**. Ce registre des traitements doit préciser les éléments suivants :

- Le ou les objectifs poursuivis par chaque traitement, ou encore appelé la **finalité.** Rappelez vous, c'est en vertu cet objectif que vous devez décider quelles données collecter.
- Les catégories de données, de personnes concernées et de personne ayant accès à ces données (équipe commerciale, logistique, hébergeur de site e-commerce etc.).
- La base légale, c'est l'élément le plus important. C'est ce qui vous autorise à prélever de la donnée personnelle. Seuls 4 cas vous y autorisent : le consentement de la personne, l'exécution du contrat avec cette personne, votre intérêt légitime ou l'obligation légale. Pour un e-commerce, vous pouvez retenir ces éléments :
- Lorsqu'une commande est passée par un client, toutes les informations pour exécuter ce contrat doivent être fondées sur cette base légale.

- Pour le reste, le consentement pour être utilisée, par exemple pour les informations relatives aux cookies sur le site.
- Si vous avez des informations sur des prospects dans votre CRM, l'intérêt légitime peut être de nature à fonder l'utilisation de ces données.
- Enfin en ce qui concerne les données que vous traitez en interne (gestion du personnel, gestion de la compatibilité etc.), en tant qu'employeur, la loi vous oblige dans de nombreuses hypothèses à collecter certaines informations. Par exemple concernant les bulletins de paie.
- Les personnes à qui peuvent être communiquées ces données (sous-traitants, prestataires). Il s'agit de toute entreprise, outil, logiciel, serveur sur lequel transitent les données personnelles. Il s'agit de lister ici les sous-traitants (étape 2 mise en conformité).
- Les durées de conservation de ces données.
- Les mesures de sécurité envisagées (mots de passe, authentification).

Exemple de traitement pour un e-commerce.

Si vous collectez les adresses postales de vos clients, voici à quoi pourrait ressembler votre traitement :

- Finalité : livraison des commandes
- Catégorie de données : adresse postale
- Personnes concernées : clients
- Personne ayant accès aux données : équipes commerciales, SAV et prestataire (par exemple Chronopost, UPS etc.)
- Base légale : le contrat
- Destinataire des données (sous-traitants) : Chronopost, UPS, Shopify, Saleforce.
- Durée de conservation : durée nécessaire au traitement (ce qui correspond à la durée du compte client). Puis suppression des données personnelles 2 ans après l'inactivité du compte client.
- Mesures de sécurité envisagées : données sauvegardées, sur nos bases de données internes hébergées sur AWS, le client est obligé de sécuriser son compte par un mot de passe d'au minimum 8 caractères, une minuscule, une majuscule et un caractère spécial.

Permettez aux personnes d'exercer leurs droits sur leurs données personnelles

En effet, leur RGPD a instauré les droits suivants :

- **Droit d'accès aux données** (article 15 RGPD),
- **Droit de rectification des données** (article 16 RGPD),
- **Droit à la portabilité des données** (article 20 du RGPD) : un internaute doit pouvoir obtenir ces données dans un format structuré, couramment utilisé et lisible par une machine,
- **Droit à l'effacement** (article 17 du RGPD) : sauf intérêt impérieux (c'est rarement le cas pour un site e-commerce), vous avez également l'obligation d'effacer ses données personnelles de vos fichiers si une personne le demande.
- **Droit d'opposition** (article 21 RGPD) : à tout moment, un internaute peut s'opposer à ce que ses données soient utilisées par vos soins pour une finalité précise. Si les données sont utilisées pour de la prospection commerciale, l'internaute peut s'y opposer sans motif. Et cela, même s'il avait au préalable donné son consentement.

Leto

Quelques bonnes pratiques pour répondre à vos obligations d'information :

- Demander aux visiteurs de votre site e-commerce **d'accepter les cookies** et leur permettre de les refuser ou de paramétrer leur choix (accepter certains traitements et pas d'autres par exemple).
- L'information doit être **intelligible par tous.** Ainsi, pour éviter des mentions trop longues au niveau d'un formulaire en ligne, garantissez un premier niveau de réponse puis proposez aux internautes un lien vers une page dédiée à la **politique de confidentialité.**
- Donnez la possibilité aux internautes **d'exercer leurs droits simplement.**

Leto à disposition un portail sur lequel les utilisateurs peuvent former leurs demandes et vous permettre de gérer toutes la procédure depuis la plateforme.

Leto

Sécurisez les données personnelles

La sécurité des données c'est un élément qui doit guider toutes les données de mise en conformité. Mais souvent, c'est celle qui demande plus de temps et plus d'attention. C'est la raison pour laquelle il s'agit souvent de la dernière étape.

La sécurité des données personnelles peut être assurée à la fois par des mesures techniques et des mesures organisationnelles.

Concernant **les mesures techniques**, c'est une attitude à adopter durant toute la vie de la donnée.

- Lors de sa collecte.

L'utilisateur a t-il la possibilité de sécuriser son compte via un mot de passe robuste ? Selon la CNIL un mot de passe robuste correspond à un minimum 8 caractères avec au moins 3 des éléments : minuscules, majuscules, chiffres et caractères spéciaux.

Leto

- Lors de sa sauvegarde et son utilisation.

Ici, ce sujet se recoupe avec celui des sous-traitants. Vous devez vous interroger sur la nationalité de l'outil à qui vous transférez des données personnelles. Attention, la localisation des serveurs n'a aucune importance. Ce qui compte c'est à le droit auquel est soumise l'entreprise et donc à son immatriculation principale. Si les données transitent par un logiciel étranger aux pays de l'Union européenne, alors de les données sont transférées en dehors de l'Europe, et souvent vers les Etats-Unis.

Leto

L’obligation de sécurité des données personnelles ne se limite pas aux données que vous récoltez mais s’étend à celles qu’utilisent vos sous-traitants. Les sites e-commerce permettent à de nombreux prestataires d’avoir accès aux données personnelles des internautes :

- Les données stockées chez **l’hébergeur de votre site e-commerce**,
- Les données détenues par les **sous-traitants logisticiens**,
- Les **marketplaces** (Fnac, Amazon, Rueducommerce …) donnent la possibilité à de nombreux e-commerçants de vendre leurs produits via la plateforme. Les acheteurs partagent ainsi leurs données personnelles à la fois avec la marketplace et avec les vendeurs auprès desquels ils passent commande.

A cette étape, il est essentiel de vérifier les risques au niveau de votre boutique en ligne, des différents processus de l’entreprise mais également des sous-traitants.

Que les données transitent par un sous-traitant ou pas, vous devez faire en sorte de protéger les données afin de réduire tout risque de violation de données (accès illégitime aux données, divulgation de données, modification non désirée ou encore disparition).

En matière de mesures organisationnelles, il s'agit ici de gouvernance au sein de l'entreprise : qui a accès à quelles données. Avez-vous correctement supprimé les accès d'anciens employés ? Les salariés ont ils une obligation de confidentialité ?

Sensibilisez vos collaborateurs à ces sujets afin de prévenir un comportement conduisant à une fuite de données personnelles.

Leto

EN CONCLUSION

Récapitulons les **étapes de mise en conformité d'un site e-commerce** :

1 Listez les données personnelles que vous collectez via votre activité e-commerce,

2 Auditez vos sous-traitants, en particulier les outils US,

3 Construisez votre registre de traitements de données personnelles,

4 Assurez l'exercice des droits de vos utilisateurs,

5 Sécurisez les données personnelles dont vous avez la charge.

CONTROLES ET AMENDES CNIL

La CNIL a utilisé son pouvoir de contrôles et de sanctions ces dernières années, notamment dans le secteur du e-commerce. Elle a effectué des contrôles autant sur place qu'en ligne.
Voici quelques exemples d'amendes suite au controle de la CNIL :

Amendes :

- **Vente de mobilier sur internet : amende de 120000€**
- **Commerce en ligne : amende de 250000€**
- **Société de commerce en ligne : amende de 35 millions d'euros**
- **Société de livraison de repas : 20000€**

Contrôles :

- **Decathlon**
- **Vinted**
- **Brico Privé**
- **Ubeeqo**

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.

Exemples de références

LEPAPE, leader du marché de la distribution de matériel sportif haut de gamme en France a choisi Leto pour l'accompagner dans sa mise en conformité, notamment afin de gérer les exercices de droits de ses clients et/ou prospects.

E-commerce engagé dans les produits d'entretien 100% naturels, SPRiNG s'est appuyé sur Leto afin de gagner à un appel d'offre qui nécessitait un registre de traitement parfaitement à jour. Ce fut un réel atout business !

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 simplifie les procédures de demandes d'exercices de droits des citoyens (salariés, clients, candidats …),

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.

LETO.LEGAL

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