Leto

SAAS ET RGPD : QUELS ENJEUX ?

NOS CONSEILS

LETO. LEGAL

SOMMAIRE

LES POINTS CLÉS

Nous aborderons dans ce livre blanc l'impact et l'importance du RGPD pour les éditeurs SaaS avant de vous détailler les différentes obligations qui incombent aux éditeurs SaaS pour une gestion des données conformes aux principes du RGPD !

QUEL IMPACT DU RGPD POUR LES EDITEURS SAAS ?

Importance du RGPD pour les éditeurs SaaS

À la différence d'un logiciel "On Premise" qui est installé directement sur les serveurs de l'entreprise qui l'utilise, le logiciel SaaS est installé sur les serveurs de l'éditeur SaaS. Par exemple, lorsque l'entreprise achète une licence Microsoft Office, Microsoft héberge en interne le logiciel. L'entreprise cliente n'a pas besoin de l'installer dans son propre système d'information.

Le SaaS allège considérablement l'entreprise cliente qui elle, paie un abonnement pour utiliser le produit.

Ainsi, c'est l'éditeur SaaS qui héberge les données à caractère personnel de son client. Ce dernier n'a la main ni sur l'exploitation du logiciel ni sur la localisation des données.

Ce peut être les données des salariés (logiciel RH) ou les données client et prospect (CRM) par exemple. A cette occasion, les fournisseurs de service collectent donc des données personnelles.

Par exemple :

- via l'identification des utilisateurs lors de la connexion : l'éditeur SaaS collecte les identifiants : nom, adresse mail, identifiant de connexion … ;
- ou pour permettre le fonctionnement de la solution, des données sont généralement saisies ou importées puis stockées. C'est le cas notamment des logiciels de paie. Pour calculer la paie et sortir un bulletin de salaire, le logiciel a besoin de nombreuses données personnelles.

Ainsi, dans le cadre d'un logiciel SaaS de très nombreuses informations personnelles circulent entre l'utilisateur et l'hébergeur. L'éditeur SaaS étant amené à traiter des données à caractère personnel pour le compte de ses clients, il est particulièrement impacté par le RGPD. Mais à quel titre ? En tant que responsable de traitement ou de sous-traitant ?

Éditeur SaaS : sous-traitant ou responsable de traitement ?

La qualification des rôles par le RGPD est très importante car elle emporte l'application de tout un régime juridique spécifique, notamment au regard des obligations et des responsabilités.
Trois rôles principaux existent : responsable de traitement, sous-traitant ou co-responsable.

- Le responsable de traitement est défini par l'article 4 du RGPD comme la personne qui détermine les finalités et les moyens du traitement. Il s'agit de la personne (morale) qui décide la manière dont vont être traitées les données personnelles.

En pratique, il s'agit des entreprises clientes et utilisatrices d'un SaaS puisqu'elles fixent l'objectif du traitement et la manière de le réaliser (nous verrons des exemples ensuite).

Leto

- Le sous-traitant est défini par l'article 4 du RGPD comme la personne qui traite des données à caractère personnel pour le compte du responsable du traitement. Le responsable de traitement lui transfère des données personnelles qu'il traite ensuite sous ses instructions.

En ce sens, le fournisseur de service SaaS (éditeur du logiciel, hébergeur) est bien sous-traitant puisqu'il traite les données pour son client et agit sous son autorité.

Toutefois, en pratique, ce n’est pas si simple ! Il faut s'intéresser à la finalité de chaque traitement pour déterminer la qualification de l’éditeur SaaS au cas par cas. Prenons l’exemple de deux finalités d’un logiciel SaaS CRM :

- **Connexion au logiciel CRM SaaS** : les données personnelles traitées au titre de la connexion des utilisateurs au logiciel par l’éditeur du logiciel le sont sous sa propre responsabilité. Pour cette finalité, l’éditeur est volontiers qualifié de responsable du traitement. En effet il s’agit de données qu’ils collectent pour son compte, ce sont des données clients.

- **Traitement des données des clients et prospects** : le logiciel de CRM est conçu de manière à traiter les données personnelles des clients et prospects pour en assurer le suivi, piloter les ventes, faciliter l’accès à l’information des différentes équipes (marketing, commercial, support). La finalité du traitement est propre à l’entreprise cliente tandis que l’éditeur met simplement le logiciel SaaS à disposition de l’entreprise. L'éditeur SaaS peut alors être qualifié de sous-traitant.

💡 Il est possible de prévoir une qualité de responsabilité conjointe de traitement. En vertu de l'article 26 du RGPD tel est le cas lorsque deux responsables du traitement ou plus déterminent ensemble et conjointement les finalités et les moyens du traitement.

Le prestataire pourra être qualifié de co-responsable du traitement plutôt que de sous-traitant pour les finalités déterminées ensemble par les parties.

C'est notamment le cas lorsque l'éditeur développe les fonctionnalités conjointement avec le client et que les deux parties assurent le support : par exemple le client assure le support fonctionnel et l'éditeur le support technique.

Cette dernière hypothèse est assez spécifique. Dans la majorité des cas, les entreprises clientes auront le statut de responsable de traitement lorsque les éditeurs de SaaS auront le statut de sous-traitant (en dehors des données personnelles qu'ils collectent pour leur compte).

Leto

SAAS ET RGPD : QUELLES SONT LES OBLIGATIONS DE L'EDITEUR ?

Dans la mesure où les éditeurs de SaaS ont le statut de sous-traitant et sont amenés à héberger un certain nombre de données personnelles pour le compte de leurs clients, il convient d'être vigilant sur plusieurs aspects.
Voici les 5 étapes à suivre pour s'assurer d'être en conformité avec le RGPD.

L'application du principe de Privacy by Design

La notion de Privacy by Design a pour objet de garantir un niveau de protection des données personnelles dès la conception du logiciel (article 25 du RGPD). Et pour un SaaS qui, par essence, met à disposition de ses clients un logiciel avec un certain nombre de fonctionnalités, ce principe est primordial.

En effet, il est recommandé de penser le produit pour :

- Proposer un nombre limité de champs. Par exemple, l'un des principes fondateurs du RGPD est le principe de minimisation des données : ne collecter que les données absolument nécessaires à l'activité. Donc par exemple, créer des formulaires utilisateurs avec des champs limités permet aux clients de ne collecter que les informations nécessaires sur les utilisateurs finaux.

- Eviter les champs "libre" qui permettent aux clients, et in fine au logiciel SaaS, de collecter n'importe quelle information. Cela permet notamment de limiter la collecte de données sensibles (opinions religieuses, origine raciale, données de santé etc.).

Rédiger un contrat sous-traitant (ou Data Processing Agreement)

C’est l’un des éléments les plus importants lorsque l’on est sous-traitant.

En qualité de sous-traitant, l’éditeur doit annexer au contrat SaaS un accord de sous-traitance de traitement de données personnelles, ou “Data Processing Agreement” (DPA) conclu avec le responsable du traitement de l’entreprise cliente. Cette obligation est imposée par l’article 28 RGPD.

Le RGPD exige que le contrat contienne un certain nombre de droits et obligations. Voici les éléments importants à retenir pour assurer une parfaite confiance de vos clients :

Leto

- **Choisissez un hébergement européen.**

C’est un élément primordial de la conformité RGPD. Il s’agit plus largement du sujet du transfert des données en dehors de l’Union européenne (UE). Tous les pays n’assurent pas une protection des données personnes équivalentes à celle du RGPD, notamment les Etats-Unis. Ainsi, le transfert de données par exemple sur AWS, Azure, Bubble etc pose pas mal de difficulté au regard de la conformité dans la mesure où la législation étasunienne permet aux autorités gouvernementales d’accéder aux données des entreprises. Si vous choisissez un hébergement US, il convient de prévoir un certain nombre de dispositifs supplémentaires afin de garantir la sécurité des données : chiffrement des données avant export, anonymisation, courte durée de conservation.

- **Mettez à disposition et à jour la liste de vos sous-traitants**

C’est l’une des obligations découlant de l’article 28 RGPD. En effet, vos clients vous transfèrent des données personnelles, vous même re-transférez ces données à vos sous-traitants en cascade. Vos clients doivent alors avoir la liste à jour de ces outils et savoir, le cas échéant, si des transferts hors UE sont opérés afin de pouvoir s’y opposer. À ce titre, vous devez prévoir une procédure permettant à vos clients de s’opposer au recours d’un sous-traitant n’offrait pas de garanties suffisantes en matière de Privacy.

- **Prévoyez des mesures techniques et organisationnelles**

Le DPA doit pouvoir informer les clients sur la manière dont vous sécurisez les données personnelles transférées. Vous devez à ce titre indiquer quelles mesures techniques ou organisationnelles sont prévues par traitement de données.

- **En cas de transfert hors UE, reprenez les clauses contractuelles types (CCT)**

Si vous êtes une entreprise située en dehors de l'UE ou si vous hébergez les données via une entreprise hors UE, sachez que l'Europe a publié des clauses contractuelles types (CCT), c'est à dire des clauses que vous pouvez reprendre en tout ou partie et vous permettant d'assurer un minimum de protection des données.

Voici les éléments les plus importants à intégrer dans votre DPA. Pour le reste, l'article 28 RGPD prévoit une liste d'autres éléments qui doivent y figurer :

- L'objet, la durée, la nature et la finalité du traitement sous-traité,
- Le type de données personnelles et leur localisation,
- Les obligations du sous-traitant ainsi que celles du client responsable de traitement (concernant l'analyse d'impact, en cas de data breach, pour l'assistance en matière d'audit etc.)
- Les instructions du responsable de traitement,

- **Élaborer la politique de confidentialité**

En qualité de responsable de traitement, l'éditeur SaaS doit établir un document répertoriant l'ensemble des informations exigées par le RGPD aux personnes dont les données sont collectées. Ces informations sont généralement mises à disposition via la politique de confidentialité qui doit, notamment, mentionner :

- L'identité du responsable de traitement et ses coordonnées ;
- Le type de données personnelles collectées ;
- La durée de conservation des données personnelles ;
- Les finalités de collecte des données personnelles ;
- La ou les bases juridiques permettant de collecter les données personnelles : il existe 6 bases légales comme le contrat ou le consentement, elles sont exclusives les unes des autres. Par exemple, si les données personnelles sont collectées au titre du contrat, vous n'avez pas besoin de recueillir le consentement de la personne concernée ;

- L’identité des destinataires des données personnelles ;
- Les mesures de sécurités prises dans le traitement des données ;
- Les droits des personnes concernées par les traitements : droit d’accès, droit à l’oubli, droit d’opposition, droit de rectification, droit à la portabilité.

💡 Si l’éditeur SaaS est co-responsable de traitement, en plus du contrat SaaS, l’article 26 du RGPD impose d’établir un accord de co-responsabilité de traitement avec le client. Celui-ci détaille les rôles de chacun et pour chaque finalité de chaque traitement.

ETABLISSEZ VOTRE REGISTRE DE TRAITEMENT DE DONNEES PERSONNELLES

Un registre de traitement de données personnelles est un document qui répertorie tout ce que vous faites des données personnelles de vos clients (responsable de traitement) et de celle que vous traitez pour votre compte.

💡 Cette obligation ne concerne pas les entreprises de moins de 250 salariés sauf exceptions :

1. Si le traitement n'est pas occasionnel comme c'est le cas pour un logiciel de gestion de la paie ou encore un logiciel CRM qui traitent des données à caractère personnel de manière régulière.
2. Si le traitement comporte un risque en termes de liberté des personnes comme par exemple un logiciel de tracking,
3. Si le traitement porte sur des données sensibles comme les données de santé, l'orientation sexuelle, l'origine raciale ou ethnique ou encore le casier judiciaire (messagerie d'entreprise, logiciel SIRH, logiciels médicaux etc).

⚠ Si le logiciel SaaS traite des données de santé, celui-ci doit obligatoirement être hébergé sur un système certifié HDS : Hébergeur de Données de Santé.

💡 Pour chaque traitement de données, les éléments suivants doivent être indiqués :

- Identités du responsable de traitement, sous-traitant et DPO (le cas échéant).
- Types de données personnelles
- Méthode de traitement des données personnelles
- Catégorie de personnes concernées,
- Liste des personnes ayant accès à ces données,
- Base légale
- Finalité
- Et mesures de sécurité associées au traitement.

Ces registres doivent être tenus à la disposition de la CNIL sur simple demande.

CHOISISSEZ UN OUTIL RGPD POUR VOUS EPAULER

Manager l’ensemble de ces données de façon manuelle est très chronophage au regard de la quantité des données collectées.

Nous vous invitons à auditer plusieurs outils et d’en choisir un en fonction de son coût, de son expérience utilisateur et de son SAV.

Sinon, il y a Leto, qui permet à tout non-juriste de pouvoir administrer automatiquement l’ensemble des données !

CONTROLES CNIL

La CNIL a utilisé son pouvoir de contrôles et de sanctions ces dernières années, notamment dans le secteur SaaS B2B. Elle a effectué des contrôles autant sur place qu'en ligne.

Voici quelques exemples d'entreprises contrôlées :

- **ALAN**
- **VOODOO**
- **CLUSTREE**
- **CEGEDIM**
- **MICROSOFT**
- **SALESFORCE**
- **PRESTASHOP**
- **DROPBOX**
- **EMAILING NETWORK**
- **IPOOME**
- **SOLWARE HOLDING**
- **IBOO**

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.

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