EDITEUR DE LOGICIEL SAAS

Quel est l'impact du RGPD sur votre activité ?
Quels sont les 6 principaux points de vigilance dans le cadre d'une mise en conformité?

Le Règlement Général sur la Protection des Données (RGPD) a un impact significatif sur les éditeurs de logiciels SaaS.

En effet, cette réglementation a instauré de nouvelles règles pour la collecte, le traitement et la protection des données personnelles, ce qui a nécessité des changements majeurs dans la manière dont ces éditeurs conçoivent leur logiciel et traitent les données de leurs utilisateurs.

Dans cette perspective, il est important de comprendre les conséquences du RGPD sur l'industrie du SaaS et les mesures que les éditeurs doivent prendre pour se conformer à cette réglementation.

Sommaire :

I. Notions : logiciel "On premise" et logiciel "Saas" - impacts.

II. Quel est le statut de l'éditeur de logiciel Saas au sens du RGPD?

III. Quels sont les principaux points de vigilance pour un éditeur de logiciel SaaS ?

I. Notions : logiciel ”On premise” et logiciel ”Saas” - Impacts

On distingue généralement deux modèles d’exploitation de logiciels : le modèle SaaS (Software as a service) et le modèle ”on premise”.

Un logiciel ”on premise” (logiciel installé localement) est un logiciel installé directement sur les serveurs de l’entreprise. Celle-ci l’utilise de manière indépendante et reste responsable de ses données et de leur sécurité. L’éditeur n’a aucun accès aux données traitées dans ledit logiciel. Il doit néanmoins fournir un logiciel conforme au rgpd.

Un logiciel ”SaaS” (logiciel en tant que service) n’est quant à lui pas hébergé sur les ordinateurs de l’entreprise mais dans le cloud. En d’autres termes, les données de l’entreprise, au lieu d’être stockées sur des disques durs ou mémoires, sont disponibles sur des serveurs distants accessibles uniquement par Internet.

Ce qui soulève un certain nombre de difficultés au regard du respect de la législation relative à la protection des données à caractère personnel.

En tant qu’éditeur de logiciel SaaS, vous êtes en effet amené à collecter et traiter des données personnelles sur vos clients. Vos clients sont par ailleurs eux-mêmes amenés à collecter et à traiter, via votre solution SaaS, des données personnelles sur leurs salariés ainsi que sur leurs propres clients ou prospects.

II. Quel est le statut de l'éditeur de logiciel SaaS au sens du Rgpd ?

Le Rgpd connait deux rôles principaux :

- Le responsable de traitement, soit la personne qui détermine les finalités et les moyens d'un traitement. En d'autres termes, la personne qui a le pouvoir de décider ce que va faire le traitement et comment il va le faire.

- Le sous-traitant, soit le prestataire qui traite des données personnelles pour le compte et sur les instructions d'un responsable de traitement.

Il existe également un statut de responsable conjoint. Cela vise l'hypothèse où deux organismes partagent la responsabilité du traitement (soit parce qu'ils conçoivent ensemble ce traitement, soit parce qu'un organisme utilise un outil développé par un éditeur et que ce dernier traite lui-même les données de ses clients par exemple à des fins internes d'amélioration de l'outil).

La qualification est importante car elle emporte l'application d'un régime spécifique, notamment en termes d'obligations et de responsabilité.

Le fournisseur de service SaaS est généralement considéré comme un sous-traitant puisque, par exemple, dans le cadre d'un logiciel SaaS CRM (logiciel de gestion de la relation client) celui-ci est conçu de manière à pouvoir traiter les données personnelles des clients et des prospects dans une optique de suivi, de pilotage des ventes, d'accès rapide à l'information, etc. La finalité du traitement est donc propre à l'entreprise cliente qui utilise le logiciel à cette fin.

Par contre, les données personnelles traitées dans le cadre de la connexion des utilisateurs au logiciel le sont sous la responsabilité de l'éditeur qui est alors qualifié de responsable de traitement. Ces données sont collectées pour son compte et constituent ses données clients.

III. Quels sont les principaux points de vigilance pour un éditeur de logiciel SaaS ?

- **1. Respecter le principe du « privacy by design » (art. 25 RGPD)**

Ce principe implique de **protéger les données à caractère personnel dès la conception du logiciel**. Il faut donc penser le logiciel de manière à ce que les différentes fonctionnalités permettent à l'utilisateur d'être en conformité avec le RGPD.

Exemples : permettre à vos clients de paramétrer par défaut et a minima la collecte de données et ne pas rendre techniquement obligatoire le renseignement d'un champ facultatif, ne collecter que les données strictement nécessaires à la finalité du traitement (minimisation des données), gérer des habilitations et droit d'accès informatiques « donnée par donnée » ou sur demande des personnes concernées, etc.

- **2. Rédiger un contrat de sous-traitance clair qui sera annexé au contrat Saas conclu avec le Responsable de traitement (art. 28 RGPD)**

Ce contrat de sous-traitance (ou Data processing agreement) doit contenir une série de mentions et d'informations prescrites par le RGPD.

- **3.Etablir un registre des activités de traitement (art. 30.2 RGPD) et documenter l'activité de sous-traitance**

En tant que sous-traitant, vous devez tenir un registre des catégories d'activités de traitement que vous effectuez pour le compte de vos clients.

Il faut en outre veiller à ce que les instructions délivrées par le responsable de traitement soient formalisées de manière écrite et procéder à leur recensement afin d'être en mesure de démontrer que vous agissez sur instruction du responsable de traitement.

- **4.Garantir la sécurité des données (art. 32 RGPD)**

Le responsable de traitement doit faire appel à un sous-traitant qui présente des garanties suffisantes en termes de sécurité et le sous-traitant doit assurer un niveau de sécurité suffisant au regard de la nature des données collectées pour le responsable de traitement.

Il est donc recommandé à l'éditeur SaaS d'élaborer une politique de sécurité des systèmes d'information ainsi que d'assurer et de documenter l'effectivité des garanties offertes par le sous-traitant en matière de protection des données (audits, certifications, etc).

Il doit également s'assurer que ses prestataires techniques (hébergeur de données, authentification, facturation, etc) soient conformes au Rgpd et prendre les mesures prescrites par le Rgpd si des données sont transférées en dehors de l'UE.

- **5.Élaborer une politique de confidentialité et un registre des traitements**

En qualité de responsable de traitement, l'éditeur Saas devra également rédiger une politique de confidentialité fournissant aux personnes concernées l'ensemble des informations exigées par le Rgpd (identité du RT, données collectées, durée de conservation des données collectées, finalités de collecte, bases juridiques, identité des destinataires, mesures de sécurités prises et droits des personnes concernées).

Si l'éditeur Saas est co-responsable de traitement, il faudra alors conclure en plus du contrat SaaS, un accord de co-responsabilité de traitement (art. 26 RGPD) avec le client.

Le registre de traitements des données personnelles est un document qui répertorie tout ce que vous faites sur les données personnelles de vos clients et sur celle que vous traitez pour votre compte.

- **6.Choisir un DPO (délégué à la protection de données).**

Pour un éditeur de logiciel Saas, cette désignation est obligatoire si le logiciel :

- permet de réaliser un suivi régulier et systématique des personnes à grande échelle, et/ou
- implique de traiter des données sensibles (comme des données de santé, des données relatives à l'appartenance syndicale, ou convictions religieuses, etc), et/ou
- implique de traiter des données relatives à des condamnations pénales et infractions.

Dans tous les autres cas, elle est recommandée. Le délégué à la protection des données constitue généralement un atout pour comprendre et respecter les obligations en matière de protection des données, dialoguer avec les autorités de contrôle et réduire les risques de contentieux et de sanctions.

Julie Lodomez
Avocate - Associée
DPO certifiée

LawellMcMiller
Bruxelles - Paris
28, Avenue Marnix - 1000 Bruxelles
Belgique
+32 2 736 40 90
https://www.lawellmcm.com/

ALTA-JURIS INTERNATIONAL
Membre du réseau Alta Juris International
https://www.altajuris.com/