Régime des sous-traitants et RGPD

Actualité législative publié le **20/06/2018**, vu **3072 fois**, Auteur : Murielle Cahen

La prise en compte du statut de sous-traitant, tant au regard de sa définition que des responsabilités en découlant, est une des mesures phares du Règlement général sur la protection des données (« RGPD »).

Le texte européen, qui a vocation à entrer en application à partir du 25 mai 2018, pousse non seulement les entreprises, mais aussi les acteurs publics concernés à vérifier et assurer leur mise en conformité d'ici là.

Si certaines dispositions demeurent presque inchangées par rapport aux textes actuellement en vigueur (on pense à la Loi informatique et Liberté de 1978, comme à la directive 95/46), d'autres naissent pratiquement avec le Règlement.

Le régime de responsabilité pleine et entière des sous-traitants, s'il en existe des prémisses au sein de la loi, fait pourtant bien partie de cette seconde catégorie : « *Avant le RGPD, il y avait une distinction relativement claire entre le responsable de traitement et le sous-traitant. Ce n'est plus le cas avec les nouvelles dispositions imposées par le RGPD* ».

De fait, c'est non seulement l'encadrement du statut même de sous-traitant qui semble être revu par le texte européen (I), mais également leur rôle quant au traitement des données qui leur incombe (II).

1. **L'encadrement du statut de sous-traitant au sein du RGPD**

Si la définition du sous-traitant est précisée par le RGPD (A), c'est non seulement pour mettre en lumière leur rôle, mais également et parallèlement les sanctions applicables en cas de manquement de leur part (B).

1. *La définition du sous-traitant*

La CNIL a pu rappeler que le sous-traitant est celui qui traite de données personnelles « *pour le compte, sur instruction et sous l'autorité d'un responsable de traitement* », comme l'indique l'article 4 du RGPD.

Dès lors, tout prestataire ayant accès à des données personnelles et les traitant dans de telles conditions relève d'un tel régime. Notez cependant que dans le cas où cette personne « *détermine la finalité et les moyens* » du traitement, elle sera qualifiée non pas de sous-traitant, mais bien évidemment de responsable de traitement.

Il sera de même, d'ailleurs, au regard des données traitées par le prestataire pour son propre compte.

À titre informatif, sachez que le G29 s'est attaché à faciliter la définition de sous-traitant en dégageant plusieurs critères pouvant constituer un faisceau d'indices, comme « *le niveau d'instruction donnée par le client au prestataire*

», le degré de contrôle du client sur ce dernier, etc.

Enfin et pour rappel, le RGPD prévoit que le statut de sous-traitant concerne aussi bien les prestataires établis au sein du territoire de l'Union européenne, que ceux basés à l'étranger, mais dont les activités visent directement des personnes ou des comportements au sein de l'Union européenne.

2. *Les sanctions en cas de manquement*

La Loi informatique et Libertés de 1978 ne prévoyait aucunement de pénaliser les manquements de ce type de prestataire. C'est désormais chose faite, à travers le RGPD, qui instaure un principe de « *responsabilisation de tous les acteurs impliqués dans le traitement des données personnelles* ».

À cette fin, l'assise de la responsabilité se base sur un régime de sanction pour les sous-traitants n'ayant pas respecté de telles obligations.

Ainsi « *toute personne ayant subi un dommage matériel ou moral du fait d'une violation du règlement européen peut obtenir la réparation intégrale de son préjudice de la part du responsable de traitement ou du sous-traitant* ».

Ces sanctions peuvent s'élever à un montant de plus de 20 millions d'euros ou, pour les entreprises, jusqu'à 4 % du chiffre d'affaires annuel mondial de l'exercice précédent.

Ces amendes se veulent incitatives pour les entreprises, et particulièrement envers celles dont le modèle économique se fonde exclusivement sur le traitement des données. La question demeure de savoir qu'elles sont les obligations des sous-traitants en la matière.

2. **Le rôle du sous-traitant en vertu du RGPD**

Certes, de nouvelles obligations incombent aux sous-traitants (A) : encore faut-il prévoir leur mise en application pratique (B), ce qui constitue tout l'enjeu à un mois de l'entrée en application du RGPD.

1. *Les obligations du sous-traitant*

L'article 28 précédemment cité souligne expressément que le sous-traitant devra « *offrir à son client des garanties suffisantes quant à la […] protection des droits de la personne concernée* ».

De ce régime général découlent plusieurs obligations pour le responsable de traitement, qui peuvent être regroupées en différentes catégories :

- Une **obligation de transparence**, qui permettra d'informer précisément le client des formalités effectuées relatives aux traitements. Tenir un registre des traitements, recenser par écrit les instructions du client, mais aussi garantir la finalité, l'étendue et la durée du traitement font partie des formalités requises à cet égard.
- Une **obligation de protection des données**, mise en œuvre par tout moyen nécessaire et dès la conception du produit ou service en question.
- Une **obligation de sécurisation des données**, assurée par la confidentialité de ces données, la notification de toute violation de celle-ci au client, ou encore la suppression des données au terme de la prestation.
- Une **obligation d'assistance**, relative à la bonne exécution du traitement, impliquant une aide au client quant au respect des droits des personnes, à la sécurité des données, ou encore quand une directive du client vous semble contraire aux textes en vigueur.

2. *La mise en œuvre de ces obligations*

Ces nouvelles dispositions rendent fort probable le manque de conformité de vos contrats. L'intégration de clauses permettant leur mise en conformité apparaît ici essentielle.

D'autre part, gardez à l'esprit que si vous êtes libre de déléguer certains traitements à un sous-traitant (après autorisation écrite de votre client), **vous devrez répondre de ses manquements** à votre client.

Sachez, par ailleurs, que si vous êtes une autorité ou un organisme public sous-traitant, ou que vous êtes amenés à traiter, pour le compte de vos clients, de données sensibles ou à grande échelle, vous avez l'obligation de désigner un délégué à la protection des données, chargé de vous accompagner dans ces tâches et de s'assurer de la conformité de ces traitements.

Enfin, dans le cas où vous êtes établi au sein de plusieurs pays de l'Union, vous bénéficiez du mécanisme de guichet unique, qui vous permet de dialoguer avec une seule autorité nationale de contrôle (en l'occurrence, celle de votre établissement principal).

Il reste moins d'un mois avant l'entrée en application du règlement général sur la protection des données. Assurez-vous donc, en tant que sous-traitant, de prendre pleinement conscience des obligations qui vous incombent d'ici là, et de celles dont vous aurez à compter de cette date.

SOURCES :

1. https://www.dpms.eu/rgpd/guide-rgpd-accompagner-sous-traitant/
2. https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf
3. http://www.privacy-regulation.eu/fr/4.htm
4. https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article28
5. https://cnpd.public.lu/content/dam/cnpd/fr/publications/groupe-art29/wp169_fr.pdf
6. https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre1 # Article3