



Le Règlement général sur la protection des données (RGPD) dans les marchés publics

Références dans les CCAG : articles 5.2 des CCAG PI, TIC, FCS, MOE, et travaux.

Les nouveaux CCAG procèdent à une actualisation pour tenir compte des règles introduites par le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (RGPD).

Néanmoins, à chaque fois que le marché a en tout ou partie pour objet un traitement de données personnelles, il sera nécessaire, pour l'acheteur, de procéder en amont de la rédaction des documents du marché à une réflexion sur l'étendue des données traitées, les finalités du traitement et les responsabilités partagées entre l'acheteur et le prestataire ; en effet, les seules clauses générales ne peuvent suffire à couvrir toutes les situations et, en présence d'un traitement de données personnelles, il sera toujours nécessaire de préciser le rôle et les responsabilités de chacun dans les documents particuliers du marché.

Il est conseillé de procéder en trois temps :

- S'interroger sur l'existence d'un traitement de données à caractère personnel
- S'interroger sur les rôles respectifs de chacun (qui est le responsable de traitement, qui est le sous-traitant ?)
- Rédiger des clauses adéquates, en fonction de l'analyse qui aura été faite de la situation.

Mon marché est-il concerné par le RGPD ?

Pour déterminer si le marché est susceptible d'être concerné par le respect du RGPD, il faut tout d'abord vérifier s'il implique de recourir ou de mettre en œuvre un traitement de données personnelles.

○ Le marché implique-t-il l'utilisation de données personnelles ?

L'article 4.1 du RGPD précise qu'une donnée personnelle est constituée par «*toute information se rapportant à une personne physique identifiée ou identifiable [...] ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments*

spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale; ».

Si certains fichiers comportent manifestement des données personnelles (comme un fichier client, une liste d'employés...), il existe des cas moins évidents comme les fichiers dits « anonymisés », mais qui permettent, par recoupement avec d'autres fichiers, d'identifier la personne concernée. Ainsi, le seul fait de supprimer des noms pour les remplacer par des pseudonymes (exemple : identifiant client), tout en conservant dans un fichier séparé la correspondance noms/pseudonymes ne permet pas de considérer que le RGPD ne s'applique pas. Il en va de même pour les fichiers où le nom des personnes concernées est supprimé, tout en conservant le numéro de téléphone ou l'adresse.

○ **Est-ce qu'il s'agit d'un traitement de données ?**

Le règlement établi un périmètre particulièrement large pour la définition du « traitement de données personnelles ». Selon l'article 4.1, il s'agit de *« toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction »*. Il n'est pas nécessaire de posséder un fichier de données personnelles pour qu'il s'agisse d'un traitement.

Ainsi, si les prestations ont pour objet de traiter des données personnelles ou que l'exécution de ces prestations nécessite le recours à des données personnelles, il sera dès lors nécessaire de déterminer les responsabilités de chacun des co-contractants (acheteur, titulaire(s) et les sous-traitants éventuels du titulaire) au regard des obligations du règlement. Si le responsable de traitement est le seul prestataire, il n'y aura pas de « partage » de responsabilité.

Définir les qualifications de l'acheteur et du prestataire

Il n'est pas possible de prévoir par contrat que le « responsable du traitement » au sens du RGPD sera le prestataire, alors même que l'acheteur tient ce rôle dans les faits. Pour savoir qui est le responsable d'un traitement mis en œuvre par un opérateur économique dans le cadre de l'exécution d'un contrat, il faut en effet effectuer une analyse du rôle de chacun en se référant aux définitions du RGPD et aux lignes directrices par le Comité Européen de la Protection des Données (CEPD) et la Commission Nationale Informatique et Libertés (CNIL). Tous les traitements mis en œuvre par les prestataires dans le cadre de marchés publics ne sont pas sous la responsabilité des acheteurs : seuls ceux qui sont visés spécifiquement, en tant qu'objet principal (voire accessoire) du marché, le sont.

A cet égard, on pourra utilement se référer aux ressources suivantes :

- le guide du sous-traitant de la CNIL : https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf
- les lignes directrices du CEPD sur la notion de responsable de traitement et de sous – traitant (en anglais) : https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en

En revanche, on pourra se référer aux termes du contrat pour analyser les rôles respectifs de chacun, en déduire des qualifications juridiques au regard du RGPD et en tirer les conséquences contractuelles qui s'imposent.

- Le responsable de traitement :

Le responsable de traitement n'est normalement pas une personne physique, mais une organisation (ex : une administration, plutôt qu'un agent nommé désigné).

Un responsable de traitement détermine les objectifs et les moyens du traitement de données. En revanche, il n'est pas nécessaire qu'il ait lui-même accès aux données traitées. Si l'administration procédant à l'achat a naturellement vocation à être le responsable de traitement des opérations menées sur des données dans le cadre d'un contrat conclu pour satisfaire ses propres besoins, on notera qu'il peut exister des cas dans lesquels cette responsabilité est assumée par le prestataire, comme par exemple dans un marché qui n'a pas pour objet de mettre en place un traitement de données à caractère , mais qui, pour son exécution, nécessite que le titulaire mette en place un traitement de données (par exemple : traitement de données intégrant les noms et coordonnées des responsables de sites administratifs à contacter dans le cadre d'un marché de construction/maintenance d'ascenseurs, de traitement de données de contact et de suivi des agents publics nécessaires à la gestion de leurs déplacements dans le cadre d'un marché portant sur l'organisation de voyages professionnels).

Il est enfin possible d'être co-responsables de traitement. Dans ce cas de figure, les deux entités déterminent conjointement les objectifs et les moyens du traitement et les responsabilités de chacun devront être précisées par les documents particuliers du marché.

- Le sous-traitant :

La notion de « sous-traitant » au sens du RGPD n'a pas la même signification qu'en droit de la commande publique. Ainsi, au sens du RGPD, le sous-traitant est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

Le sous-traitant doit :

- Être une entité séparée du responsable de traitement. Notamment, différentes directions ou services d'une même entité ne peuvent être considérées comme « séparées » et l'une ne peut donc pas être le sous-traitant de l'autre.
- Traiter les données pour le compte du responsable de traitement et sur instruction documentée; Un titulaire de marché qui met en place un traitement de données lui permettant de mieux répondre au marché ne correspond donc pas à cette définition ; tel est par exemple le cas d'un titulaire qui met en place un fichier de fournisseurs pour mieux traiter les demandes de l'acheteur à qui le titulaire doit livrer des marchandises. Dans cette hypothèse, le traitement n'est pas mis en œuvre pour le compte de l'acheteur. En revanche, si le traitement est bien mis en œuvre pour le compte de l'acheteur responsable de traitement, celui-ci peut laisser au sous-traitant une certaine latitude en choisissant la solution technique et organisationnelle la plus appropriée dans la mise en œuvre du traitement.

Établir le contrat et définir les responsabilités au regard des qualifications des acteurs

L'objectif du contrat doit être de définir les responsabilités de chacun (responsable de traitement vis-à-vis du sous-traitant, co-responsables de traitement entre eux et vis-à-vis du sous-traitant).

Le contrat devra impérativement inclure les mentions obligatoires listées aux articles 26 ou 28.3 du RGPD, en les déclinant pour la situation particulière du marché.

En tout état de cause, le contrat devra notamment définir :

- l'objet du traitement ;
- la durée du traitement ;
- la nature et la finalité du traitement ;
- le type de données à caractère personnel concernées ;
- les catégories de personnes concernées ;
- les obligations et les droits du responsable du traitement.

Point de vigilance :

Il convient de ne pas se reposer sur un « clausier RGPD » type, intégré systématiquement à chaque marché ! S'il est possible d'établir des « clauses types » pour la mise en œuvre du RGPD, il sera dans tous les cas nécessaire de les adapter à chaque marché. Il est donc indispensable de mener à chaque fois une réflexion « RGPD » afin de s'interroger sur l'existence d'un traitement de données et sur les adaptations à prévoir des clauses RGPD.