RGPD et marchés publics : les bonnes pratiques de l'ASIP Santé pour la passation et l'exécution des marchés publics

Les missions de l'ASIP Santé, inscrites dans sa convention constitutive, la conduisent à veiller à intégrer les exigences juridiques et de sécurité dès la conception des projets de systèmes d'information qui lui sont confiés. Ces exigences sont prises en compte tout au long des procédures de marchés publics, de leur passation à leur exécution. Ainsi, l'entrée en vigueur du Règlement Général sur la Protection des Données (RGPD) a conduit l'ASIP Santé à mettre en conformité avec ses dispositions tant ses procédures internes relatives à la conduite des chantiers juridiques que ses procédures de passation et d'exécution des marchés publics.

1. Mise en conformité des procédures générales de l'ASIP Santé au RGPD

▶ Délégué à la protection des données et procédures générales

Afin de prendre en compte les nouvelles obligations consacrées par le RGPD, l'ASIP Santé a notamment nommé son Correspondant Informatique et Libertés (CIL) en tant que Délégué à la Protection des Données (DPD) ou *Data Protection Officer* (DPO) depuis le 25 mai 2018. Le DPD assure :

- la conformité des traitements de données mis en œuvre par l'agence avec le RGPD ;
- le respect des droits et libertés des personnes concernées par les traitements mis en œuvre par l'agence ;
- la liaison avec le responsable de la sécurité des systèmes d'information (RSSI) pour la prise en compte de la protection des données à caractère personnel dans les procédures relatives à la gestion de risque sécurité. En outre, le RSSI de l'agence, ainsi que son adjoint, veillent également à assurer la sécurité, la disponibilité et l'intégrité des systèmes d'information (et des données) mis en œuvre par l'ASIP Santé.

L'agence disposait d'ores et déjà d'un ensemble de procédures et documentations internes visant à garantir la protection des données à caractère personnel (un registre des traitements de données, une charte informatique, un système de management de la sécurité des systèmes d'information, des outils permettant l'information des personnes concernées...). L'ensemble de ces procédures et de ce corpus documentaire est à jour du RGPD, grâce à un renforcement des mesures de protection des personnes et l'ajout de nouvelles procédures permettant de respecter les obligations introduites par le RGPD, comme la notification des violations de données à caractère personnel.

2. Passation des marchés : méthode d'élaboration du dossier de consultation des entreprises en conformité avec le RGPD

2.1 Cadrage du projet : identification des aspects relatifs au volet données personnelles

Concernant les différents projets de systèmes d'information mis en œuvre par l'ASIP Santé avec le concours d'un ou plusieurs prestataires choisis dans le cadre d'une procédure de marché public, les mesures de protection des données à caractère personnel sont définies lors du **cadrage du projet avec les différents acteurs participant au projet (ASIP Santé, prestataire(s), utilisateurs finaux, commanditaire(s) du projet, etc.).**Dans ce cadre, sont notamment déterminés :

- les mesures de sécurité adaptées au projet et au système d'information concerné ;
- l'encadrement des droits des personnes, dont les modalités d'information et de recueil du consentement, les procédures et éventuelles fonctionnalités de gestion des droits des personnes ;
- les modalités de réalisation des analyses de risques, notamment des analyses d'impact sur la protection des données ;
- les engagements et obligations spécifiques à inclure dans le dossier de consultation des entreprises (DCE).

Ce cadrage est réalisé projet par projet et est effectif au plus tard au moment de la mise en production du système d'information.

2.2 Rédaction du dossier de consultation des entreprises

2.2.1 Obligation générale d'assistance de l'ASIP Santé par le titulaire

Dans tous les dossiers de consultation des entreprises (DCE) rédigés par l'ASIP Santé, l'obligation d'assistance de l'ASIP Santé par le futur titulaire est primordiale. Ce rôle s'exerce de façon différente selon qu'il s'agisse d'un marché portant sur un système d'information particulier ou d'un marché transverse.

- Lorsque le marché porte sur un système d'information particulier (par exemple, le SI-SAMU), l'agence prévoit des unités d'œuvre spécifiques, pour permettre de procéder à des développements informatiques facilitant le respect des obligations relatives à la protection des données personnelles (par exemple, pour permettre la gestion dématérialisée de l'acceptation et de la mise à jour des conditions générales d'utilisation, la gestion intelligente de formulaires de demandes d'accès aux données, le recueil du consentement avec case à cocher et traçabilité forte de l'action, etc.).

Lorsque le marché ne porte pas sur un système d'information particulier, le travail d'identification des éventuels développements techniques à mettre en place pour satisfaire au mieux à ces obligations légales résulte d'une instruction juridique dédiée à chaque projet de système d'information dont les caractéristiques ne sont connues qu'au stade de l'exécution du marché.

En sus du DCE, des précisions peuvent être utilement apportées pour préciser l'exécution du marché sur le volet RGPD dans le plan d'assurance qualité (PAQ) et pour les exigences de sécurité dans le plan d'assurance sécurité (PAS).

2.2.2 Notions de sous-traitant au sens du RGPD et du droit de la commande publique et déclaration des relations de sous-traitance

Notions de sous-traitant au sens du RGPD et du droit de la commande publique

L'ASIP Santé veille au respect des dispositions relatives à la protection des données personnelles par ses prestataires, considérés comme des sous-traitants au sens du RGPD et de la loi Informatique et Libertés modifiée, lorsqu'ils sont amenés à traiter des données à caractère personnel.

Cette notion de sous-traitant au sens de la protection des données personnelles doit être distinguée de celle issue de la loi n° 75-1334 du 31 décembre 1975 relative à la sous-traitance (articles L.2193-1 et suivant du Code de la commande publique).

- Au sens du RGPD et de la loi Informatique et Libertés modifiée, le sous-traitant est la personne qui traite des données à caractère personnel pour le compte d'un responsable de traitement : **dans le cadre d'un marché public, le titulaire qui traite des données à caractère personnel pour le compte du pouvoir adjudicateur est ainsi, dans la plupart des cas, qualifié de sous-traitant.** Le titulaire peut lui-même sous-traiter tout ou partie du traitement à un ou plusieurs sous-traitants, sous réserve d'avoir l'autorisation du pouvoir adjudicateur, responsable de traitement.

- Au sens du droit de la commande publique et de la loi de 1975, le sous-traitant est la personne qui se voit confier tout ou une partie d'un marché public pour le compte du titulaire de ce marché.

Ces deux notions impliquent des régimes juridiques différents. Un examen au cas par cas est nécessaire selon la structure du marché :

- le pouvoir adjudicateur est généralement le responsable du traitement de données à caractère personnel occasionné par le marché. Dans certains cas, il est cependant lui-même sous-traitant du commanditaire qui a généré la passation du marché ;

- le titulaire du marché, qu'il soit seul ou en cotraitance[1] :

  - **est l'entrepreneur au sens du droit de la commande publique**, et s'il décide de sous-traiter tout ou partie du marché, auprès d'un sous-traitant au sens du droit de la commande publique, il doit le déclarer auprès du pouvoir adjudicateur via un formulaire DC4 ;

  - **est généralement le sous-traitant au sens du RGPD**, s'il traite des données à caractère personnel pour le compte du pouvoir adjudicateur (dans certains cas exceptionnels, il pourrait cependant être qualifié de co-responsable, selon l'étendue de sa mission) ;

  - **conséquence de cette répartition sur la chaine de sous-traitance :** si le titulaire décide de sous-traiter lui-même à un tiers, il doit avoir l'autorisation du pouvoir adjudicateur, responsable de traitement. Le titulaire demeure responsable auprès du pouvoir adjudicateur, responsable de traitement, des missions qu'il sous-traite.

Terminologie marchés publics	Terminologie RGPD –	Cas ASIP
Pouvoir adjudicateur	Responsables du traitement (RT)	RT ou SS-T
Titulaire	Sous-traitant (SS-T)	SS-T
Sous-traitant	Sous-traitant du sous-traitant	SS-T du SS-T

Point d'attention : la cotraitance n'entraine pas systématiquement la coresponsabilité de traitement. La coresponsabilité de traitement dépend de la répartition des rôles à l'égard uniquement du traitement des données à caractère personnel.

[1] Plusieurs opérateurs économiques peuvent choisir de répondre en groupement, également appelé cotraitance, pour mutualiser leurs moyens professionnels, techniques et financiers. À la différence de la sous-traitance, tous les membres du groupement sont en relation contractuelle avec l'acheteur et sont responsables vis-à-vis de lui.

Déclaration des relations de sous-traitance au sens des marchés publics et lien avec le RGPD

Le Titulaire a l'obligation d'informer ses propres sous-traitants des obligations de confidentialité et des mesures de sécurité qui s'imposent à lui pour l'exécution du marché. Il lui incombe de s'assurer du respect de ces obligations par ses sous-traitants.

Sur la base de ces deux régimes, l'ASIP Santé rappelle que la DAJ de Bercy a procédé à la mise à jour du DC4 au regard du RGPD, formulaire de déclaration d'un sous-traitant au sens du droit des marchés publics. Ainsi, a été insérée une nouvelle rubrique relative au traitement de données à caractère personnel. Elle doit être remplie par le Titulaire lorsque le sous-traitant se voit confier un tel traitement. Le Titulaire demeure responsable de son sous-traitant si celui-ci s'avère défaillant.

Le soumissionnaire ou titulaire coche les deux cases déclaratives (de manière cumulative) qui ont pour but de lui rappeler qu'il lui appartient de s'assurer :

- que son sous-traitant présente des garanties suffisantes pour la mise en œuvre de mesures techniques et organisationnelles propres à assurer la protection des données personnelles;

- et que le document contractuel relatif à la sous-traitance (le sous-traité) intègre les clauses obligatoires prévues par le RGPD, (notamment : autorisation écrite préalable, spécifique ou générale, délivrée par le pouvoir adjudicateur, est nécessaire au recrutement d'un sous-traitant (au sens commande publique) lorsque ce dernier est chargé de traitements de données à caractère personnel).

De plus, le titulaire est responsable de l'envoi du DC4 dans lequel il indique les activités de traitement de données à caractère personnel en question, en prenant soin de renseigner l'objet et la durée du traitement, sa nature et sa finalité, ainsi que le type de données et les catégories de personnes concernées.

A noter que dans le cadre d'un marché transverse, le DC4 pourra être mis à jour et modifié si l'instruction juridique révèle que le DC4 initial ne couvre pas l'intégralité des attentes de l'ASIP Santé en matière de protection des données à caractère personnel.

2.2.1 Obligations du titulaire

Dans le cadre de la rédaction des dossiers de consultation des entreprises (DCE), l'ASIP Santé intègre dans le contenu de ses marchés publics un ensemble de clauses définissant le cadre juridique applicable relatif au respect des règles relatives à la protection des données personnelles, en précisant la répartition des rôles des parties, l'obligation du titulaire du marché de s'y conformer, et le caractère évolutif de la clause.

Conformément aux dispositions du RGPD, les marchés publics de l'ASIP Santé imposent donc au titulaire, sous-traitant de données à caractère personnel, de respecter notamment les obligations suivantes (article 28 du RGPD) :

- le titulaire ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement ;

- il veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;

- il prend toutes les mesures requises pour assurer la sécurité du traitement ;

- il met en place un registre recensant l'ensemble des catégories d'activités de traitement effectuées pour le responsable de traitement ;

- il informe des modalités mises en œuvre pour respecter l'obligation de désigner un Délégué à la Protection des Données ;

- il assiste le responsable du traitement dans la gestion des droits des personnes, des mesures de sécurité, de la notification des violations de données à caractère personnel, et des analyses d'impact sur la protection des données, compte tenu de la nature du traitement et des informations à sa disposition ;

- il met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect de ses obligations et pour permettre la réalisation d'audits.

Dans le cadre d'un marché transverse, les mesures mises en œuvre pour garantir l'effectivité des droits des personnes, sont définies par l'ASIP Santé dans le cadre de l'analyse juridique réalisée au stade de l'exécution du marché une fois que les caractéristiques du système d'information sont définies. Ces mesures varient d'un projet à l'autre mais poursuivent le but commun de garantir les droits des personnes.

2.3 Interdiction des restrictions relatives au lieu d'exécution

Le principe de liberté d'accès à la commande publique (article 1 de l'ordonnance n° 2015-899 du 23 juillet 2015 relative aux marchés publics) interdit aux acheteurs publics d'ériger un critère géographique au rang de critère d'attribution du marché public, sauf certaines dérogations prévues dans l'ordonnance, notamment celle permettant aux acheteurs d'imposer que les moyens utilisés pour exécuter tout ou partie d'un marché public soient localiser sur le territoire des Etats membres de l'Union européenne lorsque des exigences de sécurité des informations le justifient (article 38-II de l'Ordonnance du 23 juillet 2015 relative aux marchés publics).

Ce principe n'entre pas en contradiction avec les dispositions du RGPD.

Les marchés de systèmes d'information de l'agence impliquant que des données à caractère personnel soient transmises et hébergées par le titulaire du marché sont soumis aux règles mises à jour par le RGPD, qui prévoient que les données à caractère personnelles ne peuvent être transférées en dehors de l'Union européenne qu'à la condition que le pays ou prestataire destinataire garantisse un niveau de protection suffisant.

Ce niveau de protection suffisant peut être garanti par différents outils, notamment :

- reconnaissance par la Commission européenne d'un niveau de protection suffisant dans tout le pays destinataire ;

- signature d'un contrat type de transfert de données avec l'entreprise destinataire ;

- mise en place de règles contraignantes au sein d'un groupe d'entreprises destinataires ;

- pour les Etats-Unis, auto-certification de l'entreprise destinataire.

Aussi, le RGPD n'impose pas de critère géographique qui contreviendrait aux règles de la commande publique ; le titulaire devra néanmoins satisfaire à l'une des conditions rappelées ci-dessus, afin qu'un éventuel transfert de données à caractère personnel puisse s'effectuer de façon licite (art. 44 et suivant du RGPD).

Lorsqu'il s'agit de système d'information manipulant des données de santé, il convient de préciser que le régime juridique relatif à l'hébergement des données de santé à caractère personnel fixé à l'article L. 1111-8 n'impose pas de restriction géographique.

2. Exécution des marchés : méthode de mise en conformité des marchés publics

Les obligations prévues au sein du DCE ont vocation à permettre une exécution du marché en conformité avec le RGPD.

Les équipes en charge du projet ou du système d'information ayant donné lieu au marché en cause effectuent un suivi de la bonne exécution du marché tout au long de sa durée, dans le cadre, par exemple, des instances de suivi des différents sujets, qui réunissent les équipes du pouvoir adjudicateur ainsi que les équipes du titulaire (COGRESSI pour les exigences de sécurité des systèmes d'information, etc.). Ils bénéficient d'outils leur permettant le cas échéant d'en contrôler ou en assurer la conformité (par exemple, via des audits, des demandes d'information auprès du titulaire, ou encore, le cas échéant, l'application de pénalités).

Tout au long de l'exécution du marché, des précisions peuvent être utilement apportées pour préciser certaines modalités d'exécution relatives à la protection des données à caractère personnelles, et qui peuvent être formalisées dans le plan d'assurance qualité (PAQ) et les exigences de sécurité dans le plan d'assurance sécurité (PAS).

Par ailleurs, afin d'assurer que le titulaire présente toutes les garanties de fonctionnement interne respectant les règles de la protection des données personnelles, l'ASIP Santé a pour politique de valoriser toute présentation par un candidat de certification attestant de sa politique de respect du traitement des données à caractère personnel, comme par exemple:

- les règles d'entreprise contraignantes (*Binding Corporate Rules* (BCR)) approuvées par la CNIL ;
- obtention certification ISO 27001 ;
- certification délivrée par la CNIL ;
- formulation code de conduite ;
  - marque apposée COFRAC-CNIL.

A l'issue du contrat, la réversibilité et notamment la restitution et/ou la destruction des données de l'ASIP Santé sont au cœur du suivi par les équipes.

Le chef le projet a pour responsabilité de solliciter les instructions juridiques et de sécurité, de demander l'extrait du registre du sous-traitant, le cas échéant de compléter le PAQ, veiller à ce que les titulaires fournissent les déclarations des sous-traitants (DC4), ainsi que de demander tout autre document relatif à la procédure (par exemple, si les circonstances le justifient, le chef de projet doit commander un audit permettant de veiller au respect de la conformité au RGPD).

Modalités de contrôle du titulaire du marché lorsqu'il est sous-traitant (au sens du RGPD) et sanctions

Conformément aux dispositions du RGPD, les DCE de l'agence prévoient systématiquement la possibilité pour l'ASIP Santé ou un tiers mandatés par ses soins d'effectuer des audits, lorsque le marché implique le traitement de données à caractère personnel par le titulaire.

Par ailleurs, les marchés de systèmes d'information de l'agence prévoient également une clause dédiée à l'accès aux codes sources des logiciels standards. Celle-ci prévoit que le titulaire s'assure auprès de ses éditeurs que les codes sources des logiciels standards accompagnés de l'ensemble des éléments de documentation, et, plus généralement, de l'ensemble des informations nécessaires pour en permettre l'exploitation sont régulièrement déposés, à leurs frais, auprès d'un tiers séquestre.

Enfin, concernant les sanctions prévues pour les manquements relatifs au respect du RGPD, en sus des sanctions pouvant être appliquées par les autorités de protection des données ou le juge, les marchés publics de l'agence comportent une clause de pénalités pour faute grave et peuvent par ailleurs être résiliés sur ce fondement.