

Clausier RGPD – Marché Public

Annexe 2 au CCAP Protection des données à caractère personnel

Chaque partie au contrat est tenue au respect des règles relatives à la protection des données à caractère personnel auxquelles elle a accès pour les besoins de l'exécution du contrat. Ces règles sont issues du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 ci-après désigné « le règlement européen sur la protection des données ».

La présente clause a pour objet de définir les conditions dans lesquelles le titulaire s'engage à effectuer pour le compte du pouvoir adjudicateur les opérations de traitement de données à caractère personnel définies ci-après.

1 - Obligations du pouvoir adjudicateur

Le pouvoir adjudicateur s'engage à :

- Fournir au titulaire les données visées à l'article "Description du traitement de données à caractère personnel",
- Fournir toute instruction concernant le traitement des données par le titulaire,
- Veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des données de la part du titulaire,
- Superviser le traitement, y compris réaliser les audits et les inspections auprès du titulaire.

2 - Obligations générales du titulaire

Le titulaire s'engage à :

- Traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet du présent accord-cadre
- Traiter les données conformément aux instructions documentées du pouvoir adjudicateur figurant à l'article 4.3 ou dans tout autre document ou instruction relatif au présent accord cadre provenant du pouvoir adjudicateur quel qu'en soit sa forme. Les instructions sont communiquées au fur et à mesure de l'exécution du contrat au titulaire par écrit ou sous toute forme choisie par le pouvoir adjudicateur telle que document, courrier électronique ou compte-rendu de réunion sans que cette liste ne soit exhaustive. Si le titulaire considère qu'une instruction constitue une violation du règlement européen sur la protection des données ou de toute autre disposition du droit de l'Union ou du droit des Etats membres relative à la protection des données, il en informe immédiatement le pouvoir adjudicateur. En outre, si le titulaire est tenu de procéder à un transfert de données vers un pays tiers autorisé par la CNIL ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis, il doit informer le pouvoir adjudicateur de cette obligation juridique avant le

traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

- Garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent accord-cadre.
- Veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent accord-cadre s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité et reçoivent la formation nécessaire en matière de protection des données à caractère personnel.
- Prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut.

3 - Description du traitement de données à caractère personnel

Le titulaire est autorisé à traiter pour le compte du pouvoir adjudicateur les données à caractère personnel nécessaires pour fournir les prestations objet du contrat.

Les éléments d'identification du traitement couverts par le présent accord-cadre sont les suivants :

Finalité du traitement global	Le traitement confié a pour finalité la réalisation actes de biologie médicale pour le compte des CES de l'Aisne.
Durée du traitement	Le traitement est confié sur une période allant du : 07/09/2026 au 31/12/2027
Nature des opérations de traitement confiées	Les opérations de traitement confiées sont : la réalisation d'examens sanguins et urinaires pour les patients du CES de Saint-Quentin et du CES de Laon
Type de données	Les données collectées sont : - Données personnelles du patient (nom, prénom, date de naissance, sexe, N° de Sécurité Sociale) - Données de santé - Nom du praticien prescripteur
Catégorie de personnes concernées	Les personnes concernées sont : - Les patients du CES de Saint-Quentin - Les patients du CES de Laon
Coordonnées du responsable DPO de la CPAM	dpo.cpam-aisne@assurance-maladie.fr
Responsable interne des CES pour l'exécution du présent accord-cadre	Dr Myriam GUERBAZ Directrice médicale ANPS mguerbaz@anps.net
Pour l'exécution du service objet du présent contrat, le pouvoir adjudicateur met à la disposition du titulaire les informations nécessaires suivantes :	Le CCTP de l'accord-cadre

4 - Sous-traitance des données à caractère personnel

Le titulaire peut faire appel à un sous-traitant, désigné « le sous-traitant ultérieur », pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le pouvoir adjudicateur du recours à un sous-traitant ultérieur ou de tout changement envisagé concernant l'ajout ou le remplacement de sous-traitant ultérieur. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant ultérieur et les dates du contrat de sous-traitance. Le pouvoir adjudicateur dispose d'un délai minimum de vingt et un (21) jours ouvrés à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ultérieure ne peut être effectuée que si l'acheteur n'a pas émis d'objection pendant le délai convenu.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du pouvoir adjudicateur. Il appartient au titulaire de s'assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement européen sur la protection des données. Dans tous les cas, le titulaire demeure pleinement responsable devant le pouvoir adjudicateur de l'exécution par le sous-traitant ultérieur de ses obligations.

5 - Obligation de sécurité du titulaire

Le titulaire est tenu de mettre en œuvre les mesures organisationnelles et techniques de nature à lutter contre la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

À ce titre, le titulaire met en œuvre les mesures spécifiques techniques et organisationnelles décrites dans les documents fournis au pouvoir adjudicateur dans le cadre de son mémoire technique et autres documentations transmises lors de la consultation.

Le titulaire s'engage à respecter les bonnes pratiques en matière de sécurité émises par les autorités compétentes (ANSSI, ANS et CNIL notamment) et à mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. La cartographie des risques réalisée par le titulaire pourra être présentée sur demande au pouvoir adjudicateur.

L'ensemble de ces documents devra donner lieu à modification afin de tenir compte des évolutions technologiques et des exigences réglementaires. Le titulaire a, à ce titre, une obligation de conseil envers le pouvoir adjudicateur.

Aucune modification ayant pour conséquence une régression des mesures de sécurité adoptées ne peut être portée à ces documents. Par ailleurs, toute modification envisagée devra être portée à la connaissance du pouvoir adjudicateur, sans délai et avant leur mise en œuvre. Le pouvoir adjudicateur pourra, le cas échéant, faire part de ses réserves et objections.

Le pouvoir adjudicateur pourra à tout moment solliciter le Responsable de la Sécurité des Systèmes d'Information (RSSI) et/ou le Délégué à la Protection des Données du titulaire pour s'assurer que les procédures, mesures adoptées sont appliquées et respectent les bonnes pratiques reconnues dans le domaine ainsi que les exigences du Règlement Général de Protection des Données.

6 - Flux transfrontaliers

Aucun transfert de données à caractère personnel ne peut intervenir en dehors de l'Union européenne sans l'accord préalable, exprès et écrit du pouvoir adjudicateur.

En cas d'accord du pouvoir adjudicateur, le titulaire s'engage à respecter l'ensemble des obligations en matière de transfert de données à caractère personnel vers un pays tiers et notamment à conclure un acte juridique

contraignant avec le destinataire des données comme des clauses contractuelles types, un contrat ad hoc prévoyant des garanties adéquates ou des Binding Corporate Rules (règles contraignantes d'entreprise) et d'en justifier auprès du pouvoir adjudicateur.

7 - Aide et assistance du titulaire au pouvoir adjudicateur

7.1 Droit d'information des personnes concernées

Il appartient au pouvoir adjudicateur en sa qualité de responsable de traitement de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données. Néanmoins, dans le cadre de cette obligation, le titulaire s'engage, le cas échéant, à aider et assister le pouvoir adjudicateur à s'acquitter de cette obligation et ce notamment par l'intermédiaire de mesures techniques et organisationnelles appropriées tenant compte de la nature du traitement.

7.2 Exercice des droits des personnes

Le titulaire s'engage à aider et assister le pouvoir adjudicateur par l'intermédiaire de mesures techniques et organisationnelles appropriées et en tenant compte de la nature du traitement à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits :

- droit d'accès, de rectification, d'effacement et d'opposition,
- droit à la limitation du traitement,
- droit de retirer son consentement le cas échéant,
- droit à la portabilité le cas échéant,
- droit de ne pas faire l'objet d'une décision individuelle automatisées (y compris le profilage).

Le titulaire s'engage à informer sans délai le pouvoir adjudicateur pour toute demande qu'il recevrait des personnes concernées par les opérations de traitement sous-traitées et notamment en transmettant toute demande dès réception par courrier électronique à : dpo.cpam-aisne@assurance-maladie.fr

Le titulaire s'engage à aider le pouvoir adjudicateur lors du traitement d'une réclamation d'une personne concernée et s'engage à mettre en œuvre les moyens permettant de traiter les demandes dans le délai maximal de 1 mois imposé par le règlement européen sur la protection des données.

7.3 - Sécurité des données à caractère personnel

Le titulaire est tenu d'aider et d'assister le pouvoir adjudicateur dans le cadre de la mise en œuvre des mesures techniques et organisationnelles appropriées de nature à satisfaire aux obligations de protection et de sécurisation des traitements.

Afin d'apporter une aide appropriée au pouvoir adjudicateur, le titulaire doit s'appuyer sur l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques pour les personnes concernées.

Le pouvoir adjudicateur reste le seul responsable de la mise en œuvre des propositions formulées par le titulaire.

Le titulaire informe sans délai le pouvoir adjudicateur en cas d'identification d'une vulnérabilité technique ou d'une défaillance organisationnelle.

7.4 - Notification des violations de données à caractère personnel

Le titulaire notifie au pouvoir adjudicateur toute violation de données à caractère personnel dans un délai maximum de 48 heures après en avoir pris connaissance et par le moyen suivant : Par mail à dpd.cpam-aisne@assurance-maladie.fr. Lorsque la notification n'a pas lieu dans les 48 heures, elle est accompagnée des motifs du retard.

Cette notification est accompagnée de toute documentation utile afin de permettre au pouvoir adjudicateur, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente ou encore aux personnes concernées dans les délais requis par le règlement européen sur la protection des données.

La notification contient au moins :

- la description de la nature de la violation de données à caractère personnel y compris, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises ou que le titulaire propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si, et dans la mesure où il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

7.5 - Réalisation des analyses d'impacts sur la vie privée

Le titulaire informe le pouvoir adjudicateur dès lors qu'il a connaissance d'un type de traitement qui, compte tenu de sa nature, du contexte et des finalités, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

Le titulaire s'engage à aider et assister le pouvoir adjudicateur dans la mise en œuvre de l'analyse d'impact en fournissant, à première demande, l'ensemble des informations dont le pouvoir adjudicateur a besoin pour réaliser cette analyse d'impact.

Le titulaire s'engage à aider et assister le pouvoir adjudicateur lorsque ce dernier décide de consulter l'autorité de contrôle à la suite d'une analyse d'impact ayant indiqué que le traitement présenterait un risque élevé si le traitement ne fait pas l'objet d'une modification.

Le titulaire s'engage à fournir toutes les informations qu'il dispose ainsi qu'une aide et assistance technique afin de proposer des mesures d'atténuation des risques pour les droits et libertés des personnes physiques.

8 - Sort des données à caractère personnel

Les comptes rendus signés et datés seront conservés selon la réglementation en vigueur.

Les documents leur ayant permis d'établir un diagnostic seront conservés selon la réglementation en vigueur

9 - Délégué à la protection des données

Le titulaire communique au pouvoir adjudicateur le nom et les coordonnées de son délégué à la protection des données, s'il en a désigné un conformément au règlement européen sur la protection des données ou le nom de la personne en charge de cette thématique.

10 - Registre des catégories d'activités de traitement

Le titulaire déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte du pouvoir adjudicateur comprenant :

- le nom et les coordonnées du responsable de traitement pour le compte duquel il agit, des éventuels autres prestataires et, le cas échéant, du délégué à la protection des données,
- les catégories de traitements effectués pour le compte de l'acheteur,
- le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et les documents attestant de l'existence de garanties appropriées le cas échéant,
- une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :
- la pseudonymisation et le chiffrement des données à caractère personnel;
- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;
- des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Le titulaire s'engage à maintenir à jour son registre des opérations de traitement effectuée pour le compte du pouvoir adjudicateur.

Le titulaire est tenu de justifier de l'existence de son registre à première demande du pouvoir adjudicateur ou dans le cadre d'un audit.

11 - Audit

Le pouvoir adjudicateur se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect des obligations précitées en procédant à un audit de sécurité auprès du titulaire ou en demandant communication des résultats des audits conduits en propre par le titulaire.

Le titulaire s'engage à répondre aux demandes d'audit du pouvoir adjudicateur ou d'un tiers de confiance que le pouvoir adjudicateur aura sélectionné, reconnu en tant qu'auditeur indépendant, ayant une qualification adéquate, et libre de fournir les détails de ses remarques et conclusion d'audit au pouvoir adjudicateur.

Les audits doivent permettre une analyse du respect par le titulaire de ses obligations au titre des présentes, ainsi qu'au titre de la réglementation applicable en matière de la protection des données à caractère personnel.

Le pouvoir adjudicateur doit aviser le titulaire par écrit de son intention de faire procéder à un audit moyennant le respect d'un préavis minimum de quinze (15) jours. Le pouvoir adjudicateur communique de la manière la plus précise et exhaustive possible le périmètre envisagé, la liste des opérations de contrôle et des outils de mesure qu'il envisage d'utiliser.

Le pouvoir adjudicateur communique, le cas échéant, le nom de l'auditeur. Le titulaire a le droit de refuser l'auditeur pour un motif légitime. En cas de désaccord après une troisième proposition, le choix de l'auditeur est fixé par le tribunal compétent.

Les résultats de l'audit sont formalisés dans un rapport qui doit être adressé au titulaire pour qu'il puisse y insérer ses observations et réserves. Le rapport final doit nécessairement comprendre les observations du prestataire auditeur.

Si un désaccord survient concernant des écarts de conformité, le pouvoir adjudicateur est en droit de demander une mise en conformité.

12 - Contrôle de l'autorité de protection des données personnelles (CNIL)

Le pouvoir adjudicateur et le titulaire sont tenus de coopérer avec la CNIL, à la demande de celle-ci.

Dans le cas où le contrôle mené auprès du titulaire concernerait les traitements mis en œuvre au nom et pour le compte du pouvoir adjudicateur, le titulaire s'engage à en informer immédiatement le pouvoir adjudicateur et à ne prendre aucun engagement pour lui.

En cas de contrôle de la CNIL auprès du pouvoir adjudicateur portant notamment sur les opérations de traitement sous traitées au titulaire, ce dernier s'engage à coopérer avec le pouvoir adjudicateur et à lui fournir toute information dont la CNIL pourrait avoir besoin sans délai.

Dans le cas où le contrôle mené ne concernerait que les traitements mis en œuvre par le titulaire en tant que responsable de traitement, ce dernier fait son affaire du contrôle et s'interdit de communiquer ou de faire état des données à caractère personnel du pouvoir adjudicateur.

Dans tous les cas, si le titulaire fait l'objet d'une mise en demeure, d'un avertissement ou d'une condamnation de la CNIL, même dispensée de publication, ce dernier est tenu d'en informer le pouvoir adjudicateur sans délai et au plus tard dans les 48h de la décision. Il est précisé que le titulaire en assumera seul les conséquences.

13 - Communication des données à caractère personnel à des tiers autorisés

Le titulaire s'engage à informer sans délai le pouvoir adjudicateur en cas de requête provenant d'une autorité administrative, judiciaire ou de tout tiers autorisés demandant à avoir communication de données à caractère personnel entrant dans le périmètre du présent contrat.

Dans le cas où la requête est reçue par le pouvoir adjudicateur, le titulaire s'engage à mettre en œuvre les moyens permettant de répondre à la demande dans les délais exigés sur le périmètre des opérations de traitement confiées au titulaire.

14 - Confidentialité

Le titulaire s'engage à faire signer par toutes les personnes susceptibles d'accéder aux données à caractère personnel du pouvoir adjudicateur un engagement individuel de confidentialité.

Le titulaire doit être en mesure de confirmer le respect de cette obligation auprès du pouvoir adjudicateur, à première demande, en communiquant la liste des personnes susceptibles d'accéder aux données à caractère personnel, accompagnée des engagements de confidentialité signés par lesdites personnes.

Le titulaire s'engage à former les personnes susceptibles d'accéder aux données à caractère personnel du Responsable de traitement sur les mesures de sécurité à mettre en œuvre. Le plan de formation annuel est communiqué au pouvoir adjudicateur.

Le titulaire s'engage à ce que ses éventuels sous-traitants ultérieurs soient également tenus par ces obligations spécifiques et soient en mesure d'en justifier auprès du pouvoir adjudicateur, à première demande.

Il est expressément prévu que toute modification sur ce point entre dans le cadre de l'article L2194-1 du Code de la Commande Publique. La conclusion d'un avenant ne sera pas obligatoire : la modification pourra être intégrée automatiquement à l'accord-cadre (ou du marché) sur simple information d'une partie par la partie la plus diligente.