 



**N° Consultation : CRN MP 2503**

Agence Régionale de Santé ARA

Marché de prestations intellectuelles

**Clauses contractuelles relatives à la protection des données personnelles**

* **Appel offre ouvert**

**Article L.2124-1 du code de la commande publique**

**Articles R.2124-1, R.2124-2, R.2161-2 à R.2161-5 du code de la commande publique**

# Table des matières

[1. Table des matières 2](#_Toc194474852)

[2. Objet et champ d’application 5](#_Toc194474853)

[3. Invariabilité des clauses 5](#_Toc194474854)

[4. Interprétation 5](#_Toc194474855)

[5. Hiérarchie 6](#_Toc194474856)

[6. Description du traitement 6](#_Toc194474857)

[7. Obligations des parties 6](#_Toc194474858)

[6.1. Instructions 6](#_Toc194474859)

[6.2. Limitation de la finalité 6](#_Toc194474860)

[6.3. Durée du traitement des données à caractère personnel 6](#_Toc194474861)

[6.4. Sécurité du traitement 6](#_Toc194474862)

[6.5. Données sensibles 7](#_Toc194474863)

[6.6. Documentation et conformité 7](#_Toc194474864)

[6.7. Recours à des sous-traitants ultérieurs 8](#_Toc194474865)

[6.8. Transferts internationaux 8](#_Toc194474866)

[8. Assistance au responsable du traitement 9](#_Toc194474867)

[9. Notification de violations de données à caractère personnel 10](#_Toc194474868)

[8.1. Violation de données (Responsable du traitement) 10](#_Toc194474869)

[8.2. Violation de données (sous-traitant) 11](#_Toc194474870)

[10. Non-respect des clauses et résiliation 11](#_Toc194474871)

[11. Signatures des parties 12](#_Toc194474872)

[ANNEXE I 12](#_Toc194474873)

[ANNEXE II 14](#_Toc194474874)

[ANNEXE III 15](#_Toc194474875)

*Ces clauses doivent être ajoutées uniquement si des données personnelles sont traitées. Exemples de données personnelles (source site CNIL).*

1. *Les données personnelles sont définies par l’article 4 du RGPD :* «données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; 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.

* *Lorsqu'elles sont relatives à des personnes physiques,****les données suivantes sont des données personnelles :***
  + *nom, prénom, pseudonyme, date de naissance ;*
  + *photos, enregistrements sonores de voix ;*
  + *numéro de téléphone fixe ou portable, adresse postale, adresse email ;*
  + *adresse IP, identifiant de connexion informatique ou identifiant de cookie ;*
  + *empreinte digitale, empreinte rétinienne ;*
  + *numéro de plaque d'immatriculation, numéro de sécurité sociale, numéro d'une pièce d’identité ;*
  + *données d'usage d'une application, des commentaires, etc...*
* ***L’identification des personnes physiques peut se réaliser****:*
  + *à partir d’une seule donnée (exemples : nom et prénom) ;*
  + *à partir du croisement d’un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour et membre de telle association).*
  + *Certaines données sont considérées comme****particulièrement sensibles****. Le RGPD interdit de recueillir ou d’utiliser ces données, sauf, notamment, si la personne concernée a donné son consentement exprès Ces exigences concernent les données suivantes : les données relatives à la****santé des individus****; les données concernant la****vie sexuelle****ou l'****orientation sexuelle****; les données qui révèlent une prétendue****origine raciale****ou****ethnique****; les****opinions politiques****, les****convictions religieuses****,****philosophiques****ou l'****appartenance syndicale****; les****données génétiques****et****biométriques utilisées aux fins d'identifier une personne de manière unique****.*

**ENTRE**

L’Agence régionale de santé Auvergne-Rhône-Alpes

Établissement public de l’Etat à caractère administratif

241 rue Garibaldi

CS 93383

69418 LYON CEDEX 03

Et représentée par sa Directrice générale,

(ci-après, « la responsable de traitement »)

**d'une part,**

**ET**

Nom société

Adresse

CP VILLE

SIRET : XXX

(ci-après, « le sous-traitant »)

**d’autre part,**

Vu 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 (ci-après RGPD) ;

Vu la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu le code de la commande publique

Vu l’accord-cadre n°XXX conclu le XXXX

**Il a été convenu ce qui suit,**

# Objet et champ d’application

Les présentes clauses contractuelles (ci-après les « clauses ») ont pour objet de garantir la conformité avec l’article 28, paragraphes 3 et 4, du RGPD.

La responsable du traitement et le sous-traitant précités ont accepté ces clauses afin de garantir le respect des dispositions de l’article 28, paragraphes 3 et 4, du RGPD.

Les présentes clauses s’appliquent au traitement des données à caractère personnel tel que décrit à l’annexe I.

Les annexes I à III font partie intégrante des clauses.

Les présentes clauses sont sans préjudice des obligations auxquelles la responsable du traitement est soumis en vertu du RGPD.

Elles ont pour objet de définir les conditions dans lesquelles le sous-traitant s’engage à effectuer pour le compte du responsable de traitement les opérations de traitement de données à caractère personnel définies ci-après.

Dans le cadre de leurs relations contractuelles, les parties s’engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le RGPD.

# Invariabilité des clauses

Les parties s’engagent à ne pas modifier les clauses, sauf en ce qui concerne l’ajout d’informations aux annexes ou la mise à jour des informations qui y figurent.

Elles ne sont pour autant pas empêchées d’ajouter d’autres clauses ou des garanties supplémentaires, à condition que celles-ci ne contredisent pas, directement ou indirectement, les clauses ou qu’elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées.

# Interprétation

Lorsque des termes définis respectivement dans le RGPD figurent dans les présentes clauses, ils s’entendent comme dans le règlement en question.

Les présentes clauses doivent être lues et interprétées à la lumière des dispositions du RGPD.

Les présentes clauses ne doivent pas être interprétées d’une manière contraire aux droits et obligations prévus par le RGPD ou d’une manière qui porte atteinte aux libertés ou droits fondamentaux des personnes concernées.

# Hiérarchie

En cas de contradiction entre les présentes clauses et les dispositions des accords connexes qui existent entre les parties au moment où les présentes clauses sont convenues ou qui sont conclus ultérieurement, les présentes clauses prévaudront.

# Description du traitement

Les détails des opérations de traitement, et notamment les catégories de données à caractère personnel et les finalités du traitement pour lesquelles les données à caractère personnel sont traitées pour le compte du responsable du traitement, sont précisés à l’annexe I.

# Obligations des parties

### Instructions

Le sous-traitant ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, à moins qu’il ne soit tenu d’y procéder en vertu du droit de l’Union ou du droit de l’État membre auquel il est soumis. Dans ce cas, le sous-traitant informe la responsable du traitement de cette obligation juridique avant le traitement, sauf si la loi le lui interdit pour des motifs importants d’intérêt public. Des instructions peuvent également être données ultérieurement par la responsable du traitement pendant toute la durée du traitement des données à caractère personnel. Ces instructions doivent toujours être documentées.

Le sous-traitant informe immédiatement la responsable du traitement si, selon lui, une instruction donnée par la responsable du traitement constitue une violation du règlement (UE) 2016/679 / du règlement (UE) 2018/1725 ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données.

### Limitation de la finalité

Le sous-traitant traite les données à caractère personnel uniquement pour la ou les finalités spécifiques du traitement, telles que définies à l’annexe I, sauf instruction complémentaire du responsable du traitement.

### Durée du traitement des données à caractère personnel

Le traitement par le sous-traitant n’a lieu que pendant la durée du marché, précisée à l’annexe I**.**

### Sécurité du traitement

Le sous-traitant met au moins en œuvre les mesures techniques et organisationnelles précisées à l’annexe II pour assurer la sécurité des données à caractère personnel. Figure parmi ces mesures la protection des données contre toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel ou l'accès non autorisé à de telles données (violation de données à caractère personnel). Lors de l’évaluation du niveau de sécurité approprié, les parties tiennent dûment compte de 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 sous-traitant n’accorde aux membres de son personnel l’accès aux données à caractère personnel faisant l’objet du traitement que dans la mesure strictement nécessaire à l’exécution, à la gestion et au suivi du contrat. Le sous-traitant 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.

### Données sensibles

Si le traitement porte sur des données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que des données génétiques ou des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique, ou des données relatives aux condamnations pénales et aux infractions («données sensibles»), le sous-traitant applique des limitations spécifiques et/ou des garanties supplémentaires.

### Documentation et conformité

Les parties doivent pouvoir démontrer la conformité avec les présentes clauses.

Le sous-traitant traite de manière rapide et adéquate les demandes du responsable du traitement concernant le traitement des données conformément aux présentes clauses.

Le sous-traitant met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations énoncées dans les présentes clauses et découlant directement du RGPD. À la demande du responsable du traitement, le sous-traitant permet également la réalisation d’audits des activités de traitement couvertes par les présentes clauses et y contribue, à intervalles raisonnables ou en présence d’indices de non-conformité. Lorsqu’il décide d’un examen ou d’un audit, la responsable du traitement peut tenir compte des certifications pertinentes en possession du sous-traitant.

La responsable du traitement peut décider de procéder lui-même à l’audit ou de mandater un auditeur indépendant. Les audits peuvent également comprendre des inspections dans les locaux ou les installations physiques du sous-traitant et sont, le cas échéant, effectués moyennant un préavis raisonnable.

Les parties mettent à la disposition de l’autorité de contrôle compétente, dès que celles-ci en font la demande, les informations énoncées dans la présente clause, y compris les résultats de tout audit.

### Recours à des sous-traitants ultérieurs

Le sous-traitant n’est pas autorisé à sous-traiter à un sous-traitant ultérieur les opérations de traitement qu’il effectue pour le compte du responsable du traitement en vertu des présentes clauses sans l’autorisation écrite spécifique préalable du responsable du traitement. Le sous-traitant soumet la demande d’autorisation spécifique au moins un mois avant le recrutement du sous-traitant ultérieur en question, ainsi que les informations nécessaires pour permettre au responsable du traitement de prendre une décision au sujet de l’autorisation. La liste des sous-traitants ultérieurs autorisés par la responsable du traitement figure à l’annexe IV, que les parties tiennent à jour.

Lorsque le sous-traitant recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques (pour le compte du responsable du traitement), il le fait au moyen d’un contrat qui impose au sous-traitant ultérieur, en substance, les mêmes obligations en matière de protection des données que celles imposées au sous-traitant en vertu des présentes clauses. Le sous-traitant veille à ce que le sous-traitant ultérieur respecte les obligations auxquelles il est lui-même soumis en vertu des présentes clauses et du RGPD.

À la demande du responsable du traitement, le sous-traitant lui fournit une copie de ce contrat conclu avec le sous-traitant ultérieur et de toute modification qui y est apportée ultérieurement. Dans la mesure nécessaire à la protection des secrets d’affaires ou d’autres informations confidentielles, y compris les données à caractère personnel, le sous-traitant peut expurger le texte du contrat avant d’en diffuser une copie.

Le sous-traitant demeure pleinement responsable, à l’égard du responsable du traitement, de l’exécution des obligations du sous-traitant ultérieur conformément au contrat conclu avec le sous-traitant ultérieur. Le sous-traitant informe la responsable du traitement de tout manquement du sous-traitant ultérieur à ses obligations contractuelles.

Le sous-traitant convient avec le sous-traitant ultérieur d’une clause du tiers bénéficiaire selon laquelle — dans le cas où le sous-traitant a matériellement disparu, a cessé d’exister en droit ou est devenu insolvable — la responsable du traitement a le droit de résilier le contrat conclu avec le sous-traitant ultérieur et de donner instruction au sous-traitant ultérieur d’effacer ou de renvoyer les données à caractère personnel.

### Transferts internationaux

Tout transfert de données vers un pays tiers ou une organisation internationale par le sous-traitant n’est effectué que sur la base d’instructions documentées du responsable du traitement ou afin de satisfaire à une exigence spécifique du droit de l’Union ou du droit de l’État membre à laquelle le sous-traitant est soumis et s’effectue conformément aux dispositions du RGPD.

La responsable du traitement convient que lorsque le sous-traitant recrute un sous-traitant ultérieur conformément à la clause 6.7 pour mener des activités de traitement spécifiques (pour le compte du responsable du traitement) et que ces activités de traitement impliquent un transfert de données à caractère personnel au sens du RGPD, le sous-traitant et le sous-traitant ultérieur peuvent garantir le respect des dispositions du RGPD en utilisant les clauses contractuelles types adoptées par la Commission sur la base de l’article 46, paragraphe 2, du RGPD, pour autant que les conditions d’utilisation de ces clauses contractuelles types soient remplies.

# Assistance au responsable du traitement

Le sous-traitant informe sans délai la responsable du traitement de toute demande qu’il a reçue de la part de la personne concernée. Il ne donne pas lui-même suite à cette demande, à moins que la responsable du traitement des données ne l’y ait autorisé.

Le sous-traitant prête assistance au responsable du traitement pour ce qui est de remplir l’obligation qui lui incombe de répondre aux demandes des personnes concernées d’exercer leurs droits, en tenant compte de la nature du traitement. Dans l’exécution de ses obligations, le sous-traitant se conforme aux instructions du responsable du traitement.

Outre l’obligation incombant au sous-traitant d’assister la responsable du traitement, le sous-traitant aide en outre la responsable du traitement à garantir le respect des obligations suivantes, compte tenu de la nature du traitement et des informations dont dispose le sous-traitant :

1. L’obligation de procéder à une évaluation de l’incidence des opérations de traitement envisagées sur la protection des données à caractère personnel (« analyse d’impact relative à la protection des données ») lorsqu’un type de traitement est susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques ;
2. L’obligation de consulter l'autorité de contrôle compétente préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si la responsable du traitement ne prenait pas de mesures pour atténuer le risque ;
3. L’obligation de veiller à ce que les données à caractère personnel soient exactes et à jour, en informant sans délai la responsable du traitement si le sous-traitant apprend que les données à caractère personnel qu’il traite sont inexactes ou sont devenues obsolètes ;
4. Les obligations prévues à l’article 32 du règlement (UE) 2016/679

Les parties définissent à l’annexe II les mesures techniques et organisationnelles appropriées par lesquelles le sous-traitant est tenu de prêter assistance au responsable du traitement dans l’application de la présente clause, ainsi que la portée et l’étendue de l’assistance requise.

# Notification de violations de données à caractère personnel

En cas de violation de données à caractère personnel, le sous-traitant coopère avec la responsable du traitement et lui prête assistance aux fins de la mise en conformité avec les obligations qui lui incombent en vertu des articles 33 et 34 du RGPD, selon celui qui est applicable, en tenant compte de la nature du traitement et des informations dont dispose le sous-traitant.

### 8.1. Violation de données (Responsable du traitement)

En cas de violation de données à caractère personnel en rapport avec des données traitées par la responsable du traitement, le sous-traitant prête assistance au responsable du traitement :

* aux fins de la notification de la violation de données à caractère personnel à l’autorité de contrôle compétente dans les meilleurs délais après que la responsable du traitement en a eu connaissance, le cas échéant (sauf si la violation de données à caractère personnel est peu susceptible d'engendrer un risque pour les droits et libertés des personnes physiques);
* aux fins de l’obtention des informations suivantes qui, conformément à l’article 33, paragraphe 3, du RGPD, doivent figurer dans la notification du responsable du traitement, et inclure, au moins :
  + la nature des données à caractère personnel, y compris, si possible, 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 ;
  + les conséquences probables de la violation de données à caractère personnel ;
  + les mesures prises ou les mesures que la responsable du traitement 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.

Lorsque, et dans la mesure où, il n’est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu’elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais ;

- aux fins de la satisfaction, conformément à l’article 34 du RGPD, de l’obligation de communiquer dans les meilleurs délais la violation de données à caractère personnel à la personne concernée, lorsque la violation de données à caractère personnel est susceptible d’engendrer un risque élevé pour les droits et libertés des personnes physiques.

### 8.2. Violation de données (sous-traitant)

En cas de violation de données à caractère personnel en rapport avec des données traitées par le sous-traitant, celui-ci en informe la responsable du traitement dans les meilleurs délais après en avoir pris connaissance. Cette notification contient au moins :

* une description de la nature de la violation constatée (y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et d'enregistrements de données à caractère personnel concernés);
* les coordonnées d’un point de contact auprès duquel des informations supplémentaires peuvent être obtenues au sujet de la violation de données à caractère personnel ;
* ses conséquences probables et les mesures prises ou les mesures qu’il est proposé de prendre pour remédier à la violation, y compris pour en atténuer les éventuelles conséquences négatives.

Lorsque, et dans la mesure où, il n’est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu’elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais.

Les parties définissent à l’annexe II tous les autres éléments que le sous-traitant doit communiquer lorsqu’il prête assistance au responsable du traitement aux fins de la satisfaction des obligations incombant à ce dernier en vertu des articles 33 et 34 du RGPD.

# Non-respect des clauses et résiliation

Sans préjudice des dispositions du RGPD, en cas de manquement du sous-traitant aux obligations qui lui incombent en vertu des présentes clauses, la responsable du traitement peut donner instruction au sous-traitant de suspendre le traitement des données à caractère personnel jusqu’à ce que ce dernier se soit conformé aux présentes clauses ou jusqu’à ce que le contrat soit résilié. Le sous-traitant informe rapidement la responsable du traitement s’il n’est pas en mesure de se conformer aux présentes clauses, pour quelque raison que ce soit.

La responsable du traitement est en droit de résilier le contrat dans la mesure où il concerne le traitement de données à caractère personnel conformément aux présentes clauses si :

1. le traitement de données à caractère personnel par le sous-traitant a été suspendu par la responsable du traitement et le respect des présentes clauses n’est pas rétabli dans un délai raisonnable et, en tout état de cause, dans un délai d’un mois à compter de la suspension ;
2. le sous-traitant est en violation grave ou persistante des présentes clauses ou des obligations qui lui incombent en vertu du RGPD
3. le sous-traitant ne se conforme pas à une décision contraignante d’une juridiction compétente ou de l’autorité de contrôle compétente concernant les obligations qui lui incombent en vertu des présentes clauses ou du RGPD

Le sous-traitant est en droit de résilier le contrat dans la mesure où il concerne le traitement de données à caractère personnel en vertu des présentes clauses lorsque, après avoir informé la responsable du traitement que ses instructions enfreignent les exigences juridiques applicables conformément au point 6.1 alinéa 2, la responsable du traitement insiste pour que ses instructions soient suivies.

À la suite de la résiliation du contrat, le sous-traitant supprime, selon le choix du responsable du traitement, toutes les données à caractère personnel traitées pour le compte du responsable du traitement et certifie auprès de celui-ci qu’il a procédé à cette suppression, ou renvoie toutes les données à caractère personnel au responsable du traitement et détruit les copies existantes, à moins que le droit de l’Union ou le droit national n’impose de les conserver plus longtemps. Le sous-traitant continue de veiller à la conformité aux présentes clauses jusqu’à la suppression ou à la restitution des données.

# Signatures des parties

Fait en deux exemplaires originaux à Lyon, le XX/XX/2023

|  |  |
| --- | --- |
| **L’acheteur** | **La cocontractant** |
|  | *Apposer le cachet de la société et* *porter la mention manuscrite « Lu et approuvé »* |

## ANNEXE I

**Description du traitement**

1. Catégories de personnes concernées dont les données à caractère personnel sont traitées :

A COMPLETER

1. Catégories de données à caractère personnel traitées :

A COMPLETER

1. Nature du traitement :

A COMPLETER

1. Finalité(s) pour laquelle (lesquelles) les données à caractère personnel sont traitées pour le compte du responsable du traitement :

A COMPLETER

1. Durée du traitement :

A COMPLETER

1. Pour le traitement par les sous-traitants (ultérieurs, soit l’hébergeur), préciser également l’objet, la nature et la durée du traitement :

Objet et nature du traitement : XXX

Durée du traitement : A COMPLETER

1. Sort des données

A l’issue du contrat, le sous-traitant s’engage à détruire les données au responsable de traitement.

## ANNEXE II

**Mesures techniques et organisationnelles, y compris mesures techniques et organisationnelles visant à garantir la sécurité des données : à remplir**

## ANNEXE III

Liste de sous-traitants ultérieurs (le cas échéant)

NOTE EXPLICATIVE:

La présente annexe doit être complétée en cas d’autorisation spécifique de sous-traitants ultérieurs.

La responsable du traitement a autorisé le recours aux sous-traitants ultérieurs suivants :

1.

Non-concerné

Description du traitement (y compris une délimitation claire des responsabilités dans le cas où plusieurs sous-traitants ultérieurs sont autorisés) :