

RGPD

Annexe 1 au cahier des clauses administratives particulières (CCAP)

**Accord-cadre relatif à la productions de contenus numériques : design, développement et
référencement des sites Internet .gouv.fr**

Document commun à tous les lots

Consultation n° Prod_SIG_2025_06

Contexte

L'article 28 du Règlement général sur la protection des données (RGPD) prévoit qu'un contrat ou un autre acte juridique liant le sous-traitant et le responsable de traitement (termes définis à l'article 4 du RGPD) doit être conclu. Aussi il est demandé au « *sous-traitant* » d'attester formellement sa conformité à cette annexe qui lui sera ainsi opposable.

Le Règlement UE 2016/679 a été approuvée par le Parlement européen le 14 avril 2016 et entre en application le 25 mai 2018.

La responsabilité des données personnelles s'étend désormais aux « sous-traitants (Data Processors) » en plus des « responsables de traitement (Data Controllers) ». Les entités qui traitent les données personnelles sans nécessairement agir en qualité de responsable de traitement, telles que les agences de communication ou les agences média, deviennent ainsi des entités réglementées par la RGPD.

Dans le cadre du présent accord-cadre, les termes « données à caractère personnel », « traitement », « limitation du traitement », « fichier », « responsables de traitement », « sous-traitant », « destinataire », « tiers », « consentement », « violation de données à caractère personnel », « autorité de contrôle » ont la même signification que dans 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 »).

Par « **responsable de traitement** » est entendu toute entité bénéficiaire pour le compte de laquelle est émise la commande.

NB : Le volet 2 (registre de traitement) est mis à disposition du responsable de traitement et est à renseigner par le sous-traitant.

Par « **sous-traitant** » est entendu le titulaire du présent accord-cadre, conformément au contrat passé entre l'acheteur et le titulaire de l'accord-cadre. Par exception, le titulaire peut être qualifié de responsable du traitement au sens du RGPD, pour certaines prestations, telles que précisé dans le volet n°2 de la présente annexe. Dans ce cas, les obligations de la présente annexe ne lui sont pas applicables.

Par « **sous-traitant ultérieur** » est entendu un sous- traitant du titulaire de l'accord-cadre.

Par « **données** », sont entendues, les données à caractère personnel traitées par le sous-traitant pour l'exécution des prestations mentionnées et détaillées dans le CCTP.

Par « **traitements** », sont entendus les traitements de données à caractère personnel mis en œuvre par le sous-traitant pour l'exécution des prestations mentionnées et détaillées dans le CCTP.

Cadre légal

Le sous-traitant s'engage à assurer la protection et la sécurité des données recueillies, objet du présent accord-cadre dans le respect des obligations posées par la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, du RGPD ainsi que par les législations et recommandations applicables au responsable du traitement en matière de protection des données (en particulier des données à caractère personnel) et de sécurité des systèmes d'information.

Il est rappelé qu'en cas d'atteinte à la confidentialité et à la sécurité des données à caractère personnel, la responsabilité du sous-traitant peut être engagée notamment sur la base des dispositions des articles 226-17 et 226-5 du code pénal.

Les données à caractère personnel transmises au sous-traitant ou collectées par le sous-traitant lors de l'exécution de l'accord-cadre sont couvertes par le secret professionnel (article 226-13 du code pénal) et toute violation de cette obligation engage la responsabilité pénale du sous-traitant à ce titre.

1- Statut du titulaire (« sous-traitant »)

Les parties reconnaissent que le titulaire, en sa qualité de sous-traitant, afin d'exécuter ses obligations aux termes du présent marché, aura accès et traitera les données à caractère personnel fournies par les annonceurs du groupe d'achats d'espaces en qualité de sous-traitant au sens de la réglementation visée ci-dessus.

Pour l'exécution du présent accord-cadre, le sous-traitant met en œuvre :

- Des prestations de conseil au regard de l'élaboration de traitement de données à caractère personnel ;
- Mais aussi des prestations de mise en œuvre concrète de traitement de données à caractère personnel.

Ces prestations visant à réaliser la finalité définie par les parties.

Dans ce cadre, le sous-traitant collecte, accède et analyse les données à caractère personnel pour le compte des parties en cette qualité.

Il veille, lors de l'exécution de ces prestations de conseil et de mise en œuvre, à assurer une protection des données dès la conception et par défaut conformément au règlement général pour la protection des données.

Le traitement et la nature des données précisés dans les clauses ci-après pourront être mises à jour à la signature de l'accord-cadre entre le titulaire (« sous-traitant ») et l'acheteur. Le titulaire s'engage alors à préciser ces éléments, tout comme tout autre élément devant être amendé dans le présent accord-cadre avant la mise en œuvre du traitement des données. Dans tous les cas, le titulaire (« sous-traitant ») s'engage à agir dans le respect du règlement général pour la protection des données.

2- Description du traitement

2.1 Description des activités de traitement

Dans le cadre des prestations décrites dans le CCTP, le sous-traitant doit réaliser les traitements de données suivants :

- Collecte ;
- Enregistrement ;
- Organisation ;
- Structuration ;
- Conservation ;
- Adaptation ou modification ;
- Extraction ;
- Consultation ;
- Utilisation ;
- Communication par transmission ;
- Diffusion ou toute autre forme de mise à disposition ;
- Approchement ou interconnexion ;
- Limitation ;
- Effacement ou destruction.

2.2 Détail des activités de traitement

Préalablement à la passation de toute commande impliquant un traitement de données à caractère personnel en vertu de la présente annexe, le titulaire s'engage à communiquer, à chaque responsable du traitement concerné, le détail des activités de traitement qui sont effectivement nécessaires à la réalisation de la commande, comportant au moins, pour chaque prestation nécessaire à l'exécution du bon de commande, les informations suivantes :

- Nom et description de la prestation,
- Outils utilisés,
- Typologies de données à caractère personnel et d'autres données utilisées,
- Qualification des parties en présence,
- Lieux des traitements/transferts,
- Durée des traitements,
- Catégories de personnes concernées.

Le détail des types de traitements susceptibles d'être mis en œuvre par le titulaire figure dans le volet n°2 de la présente annexe au CCAP. Ce volet n°2 est transmis par le candidat en appui de son offre et peut être actualisé à la notification via mise au point avec l'acheteur. En cours d'exécution du marché, le volet n°2 peut également être actualisé par le titulaire. Chaque entité bénéficiaire dispose alors d'un délai de 45 jours calendaires à compter de la réception de cette mise à jour pour présenter ses objections et le cas échéant refuser les modifications proposées. A défaut d'objection dans ce délai, chaque entité bénéficiaire est réputée avoir accepté en son nom la mise à jour de ce volet n°2.

Si le titulaire propose de mettre en œuvre un traitement non mentionné dans le volet n°2, il s'oblige à faire apparaître de manière très apparente cette particularité dans le cadre de son obligation de communication visée au paragraphe premier du présent article.

3- Obligations des parties

Chacune des parties s'engage à respecter la réglementation dans le cadre du présent accord-cadre.

Les responsables de traitement s'assurent que les ressources mises en œuvre dans le cadre du présent accord-cadre par le sous-traitant constitueront des garanties suffisantes de la conformité du sous-traitant et de ses services à la réglementation au regard des réponses du sous-traitant à la grille d'analyse RGPD soumise dans le cadre de l'accord-cadre.

Le titulaire s'engage à traiter les données à caractère personnel listées au présent contrat pour les seules finalités et dans les conditions convenues dans cet accord-cadre, afin de fournir les services et remplir ses obligations au titre du présent accord-cadre.

Chacune des parties tient un registre de toutes les opérations de traitement effectuées par elle. Ce registre contient au moins les informations obligatoires requises par la réglementation. Les parties mettent ce registre à la disposition de toute autorité de contrôle qui en fait la demande.

Ce registre doit contenir *a minima* les informations suivantes :

- Les finalités du traitement ;
- Les différentes catégories de données traitées ;
- Les personnes concernées par le traitement ;
- Les destinataires des données ;
- Les délais prévus de destruction des données ;
- La description des mesures de sécurité à mettre en place pour protéger les données ;
- Les garanties de sécurité supplémentaires pour les cas de transfert de données à l'international.

4- Responsabilité

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 sur instructions documentées de l'annonceur concerné et conformément aux clauses du CCTP y compris s'agissant des transferts de données vers un pays tiers ou vers une organisation internationale (le cas échéant).

Si le sous-traitant 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 les responsables de traitement. En outre, si le sous-traitant est tenu de procéder à un transfert de données vers un pays tiers 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 les responsables de traitement 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 ;
- Veiller à ce que les personnes autorisées à traiter, sous la responsabilité du sous-traitant, les données à caractère personnel pour l'exécution des prestations du présent contrat :
 - o S'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
 - o Reçoivent la formation nécessaire en matière de protection des données à caractère personnel ;

- Coopérer et assister chaque entité bénéficiaire pour leur permettre d'assurer la conformité du traitement à la réglementation et en particulier concernant les aspects suivants :
 - o La sécurité du traitement ;
 - o Les notifications de violation de données à caractère personnel ;
 - o Les analyses d'impact ;
 - o Les formalités applicables ;
 - o Les demandes d'exercice des droits réalisées par les personnes concernées ;
 - o La fourniture des documents et informations nécessaires à la satisfaction par le responsable de traitement de ses obligations.

Notification des violations de données à caractère personnel

Le titulaire de l'accord-cadre notifie à l'acheteur responsable du traitement toute violation de données à caractère personnel dans un délai maximum de 4 heures après en avoir pris connaissance, par tout moyen permettant d'attester la date et l'heure de la notification. Cette notification est accompagnée de toute documentation utile afin de permettre à l'acheteur responsable du traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

Après accord écrit de l'acheteur responsable du traitement, le titulaire de l'accord-cadre notifie à l'autorité de contrôle compétente, au nom et pour le compte de l'acheteur responsable du traitement, les violations de données à caractère personnel dans un délai maximum de huit (8) heures à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

La notification contient au moins :

- La description de la nature de la violation de 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 ;
- 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 l'acheteur 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.

S'il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

5- Sécurité et confidentialité

Le sous-traitant s'engage à respecter les principes de confidentialité énumérés à l'annexe 2 au CCAP du présent accord-cadre.

Le sous-traitant s'engage à mettre en place les mesures organisationnelles et techniques appropriées afin d'assurer la sécurité et la confidentialité des données à caractère personnel (ex.: mesures techniques, pseudonymisation, chiffrement, etc.).

Le sous-traitant, avant la mise en œuvre du traitement des données, doit préciser les mesures techniques qui doivent être effectivement mises en place dans un document référent qui les prévoit.

Plus spécifiquement, le titulaire s'engage à décrire le processus de gestion des violations de données à caractère personnel : mesures de prévention, plan de recouvrement, procédure de notification de violation de données, délai, etc.

En cas de nécessité de mettre en œuvre des diligences additionnelles, les parties conviennent de se réunir et de discuter de bonne foi des conditions de ces diligences additionnelles.

Le sous-traitant assure la sécurité et de la confidentialité des données qu'il collecte et/ou héberge pour le compte de chaque entité bénéficiaire durant toute l'exécution du présent accord-cadre, conformément aux dispositions de l'article 32 du RGPD. Il assure à chaque entité bénéficiaire la mise à disposition d'outils permettant le respect des obligations posées par la réglementation et notamment les principes de protection dès la conception et protection par défaut.

Le sous-traitant s'engage à mettre en œuvre les mesures de sécurité suivantes :

- Plan d'Assurance Sécurité (PAS)

Le sous-traitant s'engage à exécuter ses obligations en termes de sécurité des systèmes d'information.

Le sous-traitant est responsable de la rédaction initiale du PAS ainsi que de ses évolutions nécessaires pour satisfaire aux exigences de sécurité du donneur d'ordres pendant toute la durée des prestations. Le sous-traitant pourra être amené à fournir son PAS à la demande d'une entité bénéficiaire.

- Hébergement des données

Le sous-traitant communique la liste de tous les lieux de stockage de données ou assure être en capacité de localiser le lieu de stockage des données, a posteriori, en particulier suite à un incident.

Pour certaines prestations comprenant le traitement de catégories particulières de données à caractère personnel au sens de la réglementation, il peut être demandé au sous-traitant d'assurer, un hébergement exclusivement sur le sol français.

- Traçabilité

Le sous-traitant tient à la disposition de chaque entité bénéficiaire les traces de connexion aux données traitées par le personnel du sous-traitant, et ce pendant une durée conforme aux recommandations de la CNIL. Le sous-traitant informe les responsables de traitement de toute anomalie qu'il détectera dans ces traces de connexion.

- Intégrité et sauvegarde des données

Le sous-traitant s'engage à prendre les mesures nécessaires pour assurer la conservation et l'intégrité des documents et données traités pendant la durée de l'accord-cadre.

6- Sous-traitance ultérieure

Les responsables de traitement acceptent que le sous-traitant puisse faire appel à des sous-traitants ultérieurs agissant en son nom et pour son compte afin de l'assister dans les opérations de traitement des données à caractère personnel réalisées dans le cadre du présent accord. Le sous-traitant informe les responsables de traitement de tout changement prévu concernant l'ajout ou le remplacement d'un sous-traitant ultérieur donnant ainsi la possibilité aux responsables de traitement d'émettre des objections à l'encontre de ses changements.

Le sous-traitant doit conclure un contrat écrit avec tout sous-traitant ultérieur contenant les mêmes obligations que celles fixées à l'accord-cadre, notamment en leur imposant de ne traiter les données à caractère personnel des responsables de traitement que conformément aux instructions écrites du sous-traitant et de présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que les traitements répondent aux exigences de la réglementation. Nonobstant la désignation d'un sous-traitant ultérieur, le sous-traitant demeure pleinement responsable à l'égard des responsables de traitement pour tout traitement effectué par le sous-traitant ultérieur en violation des obligations du marché.

Si le recours à un ou des sous-traitants ultérieurs implique un transfert de données à caractère personnel hors de l'Espace économique européen, dans un Etat ne bénéficiant pas, pendant toute la durée du traitement, d'une décision d'adéquation au sens de l'article 45 du RGPD, le titulaire garantit que les garanties appropriées sont en place pendant toute la durée du traitement pour permettre ce transfert. A cet égard, l'entité bénéficiaire, agissant en son nom, donne mandat au titulaire pour conclure en son nom, le cas échéant, tout contrat rendu nécessaire pour mettre en place de telles garanties, telles que les clauses contractuelles types visées à l'article 46 du RGPD.

Délégué à la protection des données et Référent sécurité

Le sous-traitant communique au responsable de traitement le nom et les coordonnées de son délégué à la protection des données, s'il en a désigné un conformément à l'article 37 du règlement européen sur la protection des données.

Le sous-traitant peut utilement correspondre avec le délégué à la protection des données (DPO) et le RSSI (responsable de la sécurité des systèmes d'information) de chaque entité bénéficiaire. Le sous-traitant assure un dialogue ouvert avec ceux-ci et a une obligation de :

- Répondre à leurs éventuelles questions ;
- Fournir, le cas échéant, la documentation permettant de justifier la mise en place de mesures techniques et organisationnelles de protection appropriées concernant le traitement (mises en œuvre par lui ou par ses sous-traitants).

Des « référents données » peuvent être désignés au sein de chaque entité bénéficiaire, tel que défini ci-dessus dans la partie « contexte », afin de faciliter la coordination des actions demandées au sous-traitant notamment faisant l'objet de protocole prévoyant la coordination sur ces points entre les différents responsables de traitements et sous-traitants.

7- Registre des catégories d'activités de traitement

Le sous-traitant déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées concernant le traitement réalisé pour le compte de chaque entité bénéficiaire comprenant :

- Le nom et les coordonnées du responsable de traitement pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;
- Les catégories de traitements effectués pour le compte du responsable de traitement ;
- 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, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées ;
- Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :
 - o La pseudonymisation et le chiffrement des données à caractère personnel ;
 - o Des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
 - o 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 ;
 - o Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

8- Audits

A la demande des responsables de traitement, le sous-traitant met à disposition des responsables de traitement les rapports d'audit effectués par des organismes d'audit indépendants et toutes informations pertinentes fournies par ces organismes.

A défaut pour le sous-traitant de fournir aux responsables du traitement une preuve de sa conformité aux dispositions de l'accord-cadre via les rapports susmentionnées et/ou dans le cas où les entités bénéficiaires estiment raisonnablement nécessaire d'effectuer un audit complémentaire conformément à la réglementation et au marché, le sous-traitant accepte de se soumettre à un audit effectué par le ou les responsables de Traitement ou un auditeur indépendant réputé, ne concurrençant pas les activités commerciales du sous-traitant, dans la limite d'un audit par an. L'auditeur est choisi par l'acheteur et accepté par le sous-traitant. Il doit posséder les qualifications professionnelles requises et est soumis à un accord de confidentialité.

Sous réserve d'un incident nécessitant une intervention urgente, ces audits sont notifiés au sous-traitant au minimum quinze (15) jours en amont. Les audits sont pris en charge par le responsable de traitement.

9- Localisation et transfert des données

Le titulaire s'engage à préciser comment sont gérés la localisation et le transfert des données avant la signature de l'accord-cadre et ce conformément aux exigences requises par le RGPD.

10- Renvoi ou destruction de données à caractère personnel

Restitution des Données

Sur demande des responsables de Traitement (y incluant aux termes de la prestation) et pour quelque cause que ce soit, le sous-traitant et ses éventuels sous-contractants s'engagent à restituer sans délai aux responsables de traitement l'intégralité des données relevant de leur responsabilité dans un format structuré et couramment utilisé.

Conformément aux obligations légales et aux obligations précisées dans l'article 12.6 et 17 du CCAP, le titulaire n'est pas autorisé à détruire les documents des responsables de traitement. Si le cas échéant il souhaite le faire (archivage de données au-delà de la période légale par exemple), il ne peut le faire sans l'accord écrit de l'acheteur ou des annonceurs concernés.

Réversibilité

Le sous-traitant assure la réversibilité des prestations et s'engage à fournir :

- La documentation livrée aux termes de l'accord-cadre, qu'elle ait été produite ou collectée par le sous-traitant (modes opératoires, procédures, notice d'utilisation, base de connaissances, sauvegardes, bases de connaissances, bases de données pour le suivi des incidents, etc.) Ainsi que les conditions de livraison ;
- Les codes sources et la documentation nécessaires à la mise en œuvre des droits de propriété intellectuelle sur les résultats livrés, sur support exploitable ;
- Les modalités et les conditions de transfert de compétences/outils déployés ou développés ainsi que les ressources affectées aux prestations du marché (tout en garantissant la continuité de service jusqu'au terme du marché).

La restitution des données et de l'achèvement du processus de réversibilité est constatée par procès-verbal daté et signé par les parties. A l'issue de la prestation, une fois la restitution des données effectuée, le sous-traitant détruit les copies des données dans un délai raisonnable et doit en apporter la preuve à l'entité bénéficiaire dans un délai raisonnable suivant la signature du procès-verbal de restitution et d'achèvement du processus de réversibilité, à moins que le sous-traitant ne soit légalement tenu de conserver les Données (si tel est le cas le sous-traitant est tenu d'en informer le responsable de traitement).