

Clauses contractuelles entre l'Agence française de lutte contre le dopage et ses sous-traitants relatives à la protection des données à caractère personnel

ANNEXE n° 1 AU CCAP

CLAUSES PARTICULIERES A LA PROTECTION DES DONNEES PERSONNELLES

I - Objet

Dans le cadre de l'exécution du marché public, le titulaire du marché sera amené à avoir accès et traiter des données à caractère personnel, au sens du Règlement Général sur la Protection des Données (EU) 2016/679 (ci-après « les données »), pour le compte de l'Agence française de lutte contre le dopage (l'AFLD).

Dans le cadre de la mise en œuvre de ce traitement de données à caractère personnel, l'AFLD est le responsable du traitement et le titulaire du marché sera le sous-traitant au sens du Règlement. Dès lors, les dispositions suivantes ont pour objectif d'encadrer les droits et obligations de chacune des parties au cours du traitement de données à caractère personnel tel que l'impose l'article 28. 3 du Règlement. Le terme de sous-traitant en droit des données personnelles est à ne pas confondre avec le terme de sous-traitant au sens de la réglementation de la commande publique.

II – Description du traitement

Le traitement ainsi réalisé par le titulaire du marché, pour le compte de l'AFLD, répond aux caractéristiques suivantes :

- **Nature des opérations réalisées sur les données** : l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, l'effacement ou la destruction.
- **Finalité(s) du traitement** : Le titulaire dispose d'outils informatisés permettant la réalisation des prestations définies dans le cadre du marché.

Catégories de données traitées : données personnelles relatives aux personnes concernées par les prestations du marché, y compris données personnelles de santé

III – Obligation du titulaire du marché vis-à-vis de l'AFLD

Le titulaire du marché s'engage à :

1. Traiter les données uniquement pour la ou les seule(s) finalité(s) nécessaire à la réalisation des prestations et conformément aux instructions documentées de l'AFLD. Si le titulaire du marché considère qu'une instruction constitue une violation du Règlement (UE) 2016/679 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 l'AFLD ;

2. Ne réaliser aucun transfert des données hors de l'Espace Economique Européen, au sens de la réglementation applicable, sauf à recueillir le consentement préalable et exprès de l'AFLD ;

3. Garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent contrat.

4. Veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent contrat :

- S'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
- Reçoivent la formation nécessaire en matière de protection des données à caractère personnel ;
- S'engagent à respecter les consignes de sécurité de l'AFLD ;

5. 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.

6. Pouvoir d'instruction de l'AFLD

Le titulaire du marché est tenu à tout moment de respecter les instructions générales et spécifiques de l'AFLD relatives au traitement des données. Le titulaire du marché s'engage à fournir sur demande de l'AFLD les informations requises aux fins de permettre un contrôle effectif de l'AFLD des modalités de traitement des données et à rendre disponible la documentation s'y rapportant.

7. Sous-traitance ultérieure

Le titulaire du marché ne peut transmettre de données à des tiers (ci-après « sous-traitant ultérieur ») qu'avec l'autorisation écrite, préalable et spécifique de l'AFLD. Ces activités de traitements sous-traitées doivent être clairement indiquées dans la déclaration de sous-traitance (DC4) soumise à l'approbation du responsable de traitement.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions de l'AFLD. Il appartient au titulaire du marché 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 (UE) 2016/679. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le titulaire du marché demeure pleinement responsable devant l'AFLD l'exécution par l'autre sous-traitant de ses obligations.

8. Exercice des droits des personnes

Dans la mesure du possible, le titulaire du marché doit aider l'AFLD à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées.

Lorsque les personnes concernées exercent auprès du titulaire du marché des demandes d'exercice de leurs droits, celui-ci doit adresser ces demandes dès réception par courrier électronique à l'adresse :

(à définir par le titulaire)

9. Ne divulguer les données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;

10. Ne faire aucune copie des données.

11. Notification des violations de données à caractère personnel

Le titulaire informe conjointement le délégué à la protection des données et le responsable de la sécurité des systèmes d'information de l'AFLD, sans délai, de toute violation de données à caractère personnel visées au II des présentes clauses (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 gérées par le sous-traitant pour le compte de l'AFLD ou l'accès non autorisé à de telles données). Cette information est complétée, dans les meilleurs délais, à partir de la fiche type « incident de sécurité », annexée aux présentes clauses, accompagnée de toute documentation utile et transmise de manière sécurisée.

12. Délégué à la protection des données et registres des catégories d'activités de traitement

Dans la mesure où le titulaire du marché aurait désigné un délégué à la protection des données, il s'engage à en communiquer le nom et les coordonnées à l'AFLD. Par ailleurs, le titulaire du marché déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte de l'AFLD, comprenant l'ensemble des informations requises en application de l'article 30 (2) du Règlement (UE) 2016/679.

13. Sort des données

Au terme de l'exécution du marché, le titulaire du marché s'engage à détruire toutes les données à caractère personnel. Une fois détruites, le titulaire doit justifier par écrit de la destruction.

14. Mesures de sécurité

Le titulaire s'engage à mettre en place des mesures de sécurité organisationnelles ainsi que des mesures de sécurité techniques appropriées pour préserver la sécurité et l'intégrité des données personnelles et les protéger contre toute déformation, altération, destruction fortuite ou illicite, endommagement, perte, divulgation ou accès à des tiers non autorisés.

Le titulaire du marché s'engage à mettre en œuvre les mesures de sécurité suivantes :

- La conservation sécurisée des données au sein de ses locaux et de ses supports informatiques ;
- Les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes de la plateforme de génération de carte professionnelle.
- Des mesures de sécurité logique visant à protéger les informations hébergées et traitées (architectures de filtrage et de protection réseau, renforcement de la protection des serveurs et postes de travail, authentification des collaborateurs pour leur conférer des profils d'utilisation conformes au principe de moindre privilège et respectant le besoin d'en connaître, mesures renforcées pour l'accès aux fonctions de gestion des données et d'administration du système d'information) ;
- Des protocoles de gestion des habilitations associés à des dispositifs permettant de tracer l'ensemble des actions réalisées sur le système d'information dans le cadre d'opérations de support et de maintenance ;

Le titulaire s'engage à maintenir ces mesures et moyens pour toute la durée du marché et à défaut, à en informer immédiatement l'AFLD.

En tout état de cause, le titulaire du marché s'engage, en cas de changement des moyens visant à assurer la sécurité, l'intégrité et la confidentialité des données personnelles, à les remplacer par des moyens équivalents à l'état de l'art ou d'une performance supérieure.

15. Documentation

Le titulaire du marché met à la disposition de l'AFLD la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par l'AFLD ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

IV - Obligation de l'AFLD vis-à-vis du titulaire du marché

L' AFDL s'engage à :

1. Fournir au titulaire du marché les données visées au II.
2. Documenter par écrit toute instruction concernant le traitement des données par le titulaire du marché
3. 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 du marché
4. Superviser le traitement, y compris réaliser les audits et les inspections auprès du titulaire du marché

Annexe : fiche incident de sécurité

PARTIE I : Contexte

- Source de la détection :

Service, agent, outil de sécurité, source extérieure...

- Date de la détection :

Cliquez ici pour entrer une date.

- Personne en charge du
traitement de l'incident :

Préciser la personne et le service qui pilotent et qui
contribuent à la prise en charge de l'incident.

- Levée de doute :

La levée de doute est initiée sans délai par le sous-
traitant avec l'appui de la CNIL, le cas échéant.
La levée de doute doit permettre de répondre, si
possible, aux questions quoi ? qui ? auprès de qui ?
quand ?

- Description générale :

Expliquer le problème, préciser tous les éléments
utiles à la qualification de la nature du risque.

En particulier :

- 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 d'un point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- la description des conséquences probables de la violation de données à caractère personnel ;

PARTIE II : Origine(s) de l'incident

Détailler la recherche de l'incident, les éléments analysés, les éventuelles sources intéressantes (journaux d'évènements, articles de presse, copies d'écran...)

- Méthodes d'analyse :

Présenter les résultats de l'analyse en précisant la/les causes avérées/possibles de l'incident.

- Résultats de l'analyse :

PARTIE III : Mesure(s) prise(s)

Présenter en détail les mesures techniques et organisationnelles mises en œuvre immédiatement pour corriger ou limiter l'incident et en prévenir toute nouvelle survenance, en particulier la description des mesures prises ou que le sous-traitant 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.

Présenter également les mesures prises en complément des mesures immédiates afin que des incidents similaires ne puissent pas se reproduire à l'avenir.