

Annexe 1 au CCAP : Clauses RGPD

1. Obligations en matière de traitement des données à caractère personnel

1.1 Obligations du Titulaire

1.1.1 Respect des finalités du traitement et des instructions indiquées dans le CCAP

Le Titulaire s'engage à traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/ont l'objet de la sous-traitance, et à traiter les données conformément aux instructions données par l'EFS et indiquées au présent CCAP.

Si le Titulaire considère qu'une instruction constitue une violation du RGPD 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'EFS par tous moyens permettant d'assurer une réception certaine.

Si le Titulaire 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 européenne, ou du droit de l'Etat membre auquel il est soumis, il doit en informer l'EFS par tous moyens permettant d'assurer une réception certaine avant le transfert, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

1.1.2 Confidentialité des données personnelles

Le Titulaire garantit la confidentialité des données à caractère personnel traitées dans le cadre du présent marché public.

A cette fin, le Titulaire s'engage à :

- ne prendre aucune copie des documents et/ou supports d'informations qui lui seraient confiés, à l'exception des copies nécessaires pour les besoins de l'exécution des Services objets du présent marché public, et à la condition que l'EFS ait donné son accord préalable ;
- ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées au présent marché public ;
- ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales ;
- prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution du marché public.

Le Titulaire veille à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent marché public :

- 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.

1.1.3 Protection des données dès la conception et protection des données par défaut

Le Titulaire prend 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 (en garantissant que seules les données nécessaires à la finalité du traitement au regard de la quantité de données collectées, de l'étendue du traitement, de la durée de conservation et du nombre de personnes qui y a accès).

1.1.4 Droit d'information des personnes concernées

Il appartient à l'EFS de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

1.1.5 Exercice des droits des personnes

Le Titulaire assiste l'EFS sur toute demande circonstanciée pour s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

Lorsque les personnes concernées exercent auprès du Titulaire des demandes d'exercice de leurs droits, le Titulaire adresse ces demandes dès réception par courrier électronique à **efs.dpo@efs.sante.fr**

1.1.6 Notification des violations de données à caractère personnel

Le Titulaire notifie à l'EFS toute violation de données à caractère personnel dans un délai maximum de 48 heures après en avoir pris connaissance et par le moyen suivant : **efs.dpo@efs.sante.fr**

Cette notification est accompagnée de toute documentation utile afin de permettre à l'EFS, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

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 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.

1.1.7 Assistance du Titulaire dans le cadre du respect par le responsable de traitement de ses obligations

Le Titulaire assiste l'EFS pour la réalisation d'analyses d'impact relative à la protection des données et lui fournit toute information nécessaire au respect des obligations qui lui incombent au titre du règlement européen sur la protection des données.

Le Titulaire assiste l'EFS pour la réalisation de la consultation préalable de l'autorité de contrôle.

1.1.8 Mesures de sécurité

Le Titulaire met en œuvre les mesures de sécurité suivantes et toute autre mesure rendue nécessaire à l'issue de l'éventuelle l'analyse d'impact relative à la protection des données réalisée par l'EFS responsable de traitement :

- *la pseudonymisation et le chiffrement des données à caractère personnel*
- *les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;*
- *les 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).*

1.1.9 Sort des données

Au terme du présent marché public, le Titulaire s'engage à renvoyer toutes les données à caractère personnel au responsable de traitement. Le renvoi doit s'accompagner de toutes les copies existantes dans les systèmes d'information du Titulaire.

1.1.10 Délégué à la protection des données

Si, en application de l'article 37 du RGPD, le Titulaire a désigné un délégué à la protection des données, il en communique le nom et les coordonnées à l'EFS.

1.1.11 Registre des catégories d'activités de traitement

Le Titulaire tient par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte de l'EFS comprenant :

- le nom et les coordonnées de l'EFS pour le compte duquel il agit, des éventuels sous-traitants de rang ultérieur et, le cas échéant, du délégué à la protection des données ;
- les catégories de traitements effectués pour le compte de l'EFS ;
- 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 RGPD, les documents attestant de l'existence de garanties appropriées ;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles définies supra.

1.1.12 Documentation

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

L'EFS se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect des obligations précitées.

1.2 Obligations de l'EFS, responsable de traitement, à l'égard du Titulaire

L'EFS s'engage à :

- fournir au Titulaire les données visées au présent CCAP ;
- documenter par écrit 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 RGPD de la part du Titulaire ;
- superviser le traitement, y compris réaliser les audits et les inspections auprès du Titulaire.

1.3 Sous-traitance au sens de la loi Informatique et libertés

L'EFS, responsable de traitement de données à caractère personnel, dispose d'un délai de 21 jours à compter de la date de réception de la déclaration de sous-traitance cette information pour présenter ses objections.

Cette sous-traitance ne peut être effectuée que si le responsable de traitement n'a pas émis d'objection pendant le délai convenu.

En cas de sous-traitance de second rang, le Titulaire doit recueillir l'autorisation écrite, préalable et spécifique de l'EFS, responsable de traitement.

Le sous-traitant de second rang est tenu de respecter les obligations du présent marché public pour le compte et selon les instructions de l'EFS. Il appartient au Titulaire de s'assurer que le sous-traitant de second rang 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 RGPD. Si le sous-traitant de second rang ne remplit pas ses obligations en matière de protection des données, le Titulaire demeure pleinement responsable devant l'EFS de l'exécution, par le sous-traitant de second rang, de ses obligations.

2. Protection des données personnelles

Dans le cadre de l'exécution du présent marché public, l'EFS et le Titulaire s'engagent à respecter le droit en vigueur applicable au traitement de données à caractère personnel et, en particulier, le RGPD.

Le présent article définit les conditions dans lesquelles le Titulaire s'engage à effectuer pour le compte de l'EFS les opérations de traitement de données personnelles définies ci-après.

L'EFS entend confier au Titulaire, pour son compte et sous sa responsabilité, le Traitement de données personnelles dont il est responsable.

Le Titulaire s'engage à disposer, pour l'EFS, des garanties suffisantes concernant la mise en œuvre de mesures techniques et organisationnelles appropriées afin que le traitement dont il a la responsabilité réponde aux exigences du RGPD.

Le Titulaire est autorisé à traiter pour le compte de l'EFS les données à caractère personnel nécessaires pour fournir le ou les service(s) suivant(s) : Fourniture de véhicules neufs en location longue durée sans chauffeur et prestations associées pour les établissements de l'EFS et prestations associées.

La nature et finalité des opérations réalisées sur les données est la collecte de données concernant les personnels de l'EFS pour le paramétrage nécessaire à l'utilisation des véhicules.

Les données à caractère personnel traitées sont : Nom, prénom, fonction, matricule, immatriculation du véhicule.

Les catégories de personnes concernées sont : Personnel de l'EFS

Pour l'exécution des prestations, l'EFS met à la disposition du titulaire du marché les informations nécessaires suivantes : Nom, prénom, fonction, matricule, immatriculation du véhicule.