

Protection des données à caractère personnel

Mise en conformité avec la loi « informatique et libertés » du 6 janvier 1978 modifiée et le règlement (UE) 2016/679 du Parlement et du Conseil du 27 avril 2016

Annexe n° E au cahier des clauses administratives particulières

Pour l'application des présentes, au sens du 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, et abrogeant la directive 95/46/CE (ci-après, « **règlement général sur la protection des données** », RGPD), **le responsable de traitement, est l'acheteur public et le sous-traitant est le titulaire du marché public.**

A. Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le titulaire s'engage à effectuer pour le compte de l'acheteur, les opérations de traitement de données à caractère personnel dans les conditions définies ci-après.

B. Description du traitement des données à caractère personnel nécessaires à l'exécution du marché

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 règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (ci-après, « **le règlement européen sur la protection des données** »).

Le titulaire est autorisé à traiter pour le compte de l'acheteur responsable de traitement des données à caractère personnel nécessaires pour fournir le ou les service(s) suivant(s) :
« **Prestation liées à l'exploitation de la résidence hôtelière du site de Cazaux de la Direction Générale de l'Armement (DGA EV)** ».

- a) La nature des opérations réalisées sur les données est [...].
- b) La ou les finalité(s) du traitement sont [...].
- c) Les données à caractère personnel traitées sont [...].
- d) Les catégories de personnes concernées sont [...].

Pour l'exécution des prestations objets des présentes, l'acheteur met à la disposition du titulaire les informations nécessaires suivantes [...].

C. Durée de l'engagement des parties

Les présentes clauses entrent en vigueur à compter de la notification du marché (ou de l'avenant, le cas échéant) par l'acheteur au titulaire pour toute la durée d'exécution du marché.

D. Obligations du titulaire vis-à-vis de l'acheteur

I. Confidentialité des données

Le titulaire s'engage à :

- a) Traiter les données **uniquement pour la ou les seule(s) finalité(s)** qui fait/font l'objet du présent marché.
- b) Traiter les données **conformément aux instructions documentées de l'acheteur (article VII du présent document et articles 12 et 13 du CCAP).**

En outre, 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 ou du droit de l'État membre auquel il est soumis, il doit informer immédiatement l'acheteur de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public. Il ne doit pas procéder au transfert des données sans avoir obtenu l'autorisation préalable de l'acheteur.

- c) **Garantir la confidentialité** des données à caractère personnel traitées dans le cadre des présentes clauses.
- d) Veiller à ce que les **personnes autorisées à traiter les données à caractère personnel** en vertu des présentes clauses :
 - 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.
- e) **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.**

II. Sous-traitance de niveau 2 ou sous-traitance ultérieure des activités de traitement

Le titulaire du marché peut faire appel à un sous-traitant (ci-après, « le sous-traitant ultérieur ») pour mener des activités de traitement clairement identifiées. Dans ce cas, il informe préalablement et par écrit l'acheteur de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant, les dates de notification du marché (ou le cas échéant de l'avenant) et les dates du contrat de sous-traitance. L'acheteur dispose d'un délai minimum de **15 jours** à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si l'acheteur n'a pas émis d'objection pendant le délai convenu.

Afin d'obtenir l'acceptation et l'agrément de l'acheteur, le titulaire doit présenter son sous-traitant (tant aussi bien au sens du RGPD, que du sens de la loi n°75-1334 du 31 décembre 1975 relative à la sous-traitance) par le biais de l'acte spécial de sous-traitance, dont les formalités

sont comprises dans le formulaire DC4 ou tout autre document équivalent (téléchargeable sur <http://www.economie.gouv.fr/daj/formulaires-declaration-candidat>).

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte de l'acheteur. 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 européen sur la protection des données. 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'acheteur de l'exécution par l'autre sous-traitant de ses obligations.

III. Droit d'information des personnes concernées

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

IV. Exercice des droits des personnes

Le titulaire doit aider l'acheteur à 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).

La formulation et le format de l'information doivent être convenus avec l'acheteur avant la collecte des données.

V. Notification des violations des données à caractère personnel

Le titulaire notifie à l'acheteur toute violation de données à caractère personnel dès qu'il en a connaissance et dans un délai maximum de 72 heures, par le moyen suivant **par courriel ou par courrier postal**. Cette notification est accompagnée de toute documentation utile afin de permettre à l'acheteur, si nécessaire, de notifier cette violation au délégué à la protection des données du ministère des armées. Le titulaire est tenu de communiquer à l'acheteur toute information complémentaire, nécessaire à la notification.

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 ;
- ♣ 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.

La notification des violations est transmise à la CNIL par le délégué à la protection des données du ministère des armées.

Lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, la notification de ladite violation est communiquée à la personne concernée par l'administration (responsable de traitement).

VI. Analyse d'impact

Le titulaire aide l'acheteur pour la réalisation d'analyses d'impact relative à la protection des données.

Le titulaire conseille l'acheteur en cas de consultation de la CNIL sur l'analyse d'impact réalisée. Cependant, celle-ci est présentée à la CNIL par le délégué à la protection des données du ministère des armées.

VII. Mesures de sécurité des données

Le titulaire met en œuvre les mesures de sécurisation des données nécessaires.

- *les droits d'accès aux données sont limités ;*
- les mesures de sécurité prévues au CCTP et CCAP.

VIII. Detenir des données au terme de l'exécution du marché

Au terme de l'exécution du présent marché, le titulaire s'engage à :

- Ne pas conserver les données à caractère personnel ;
- Renvoyer toutes les données à caractère personnel à l'acheteur.

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du titulaire. Une fois détruites, le titulaire doit justifier par écrit de la destruction. (planning, plan etc...)

IX. Délégué à la protection des données

Le titulaire communique à l'acheteur **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 ou, à défaut, l'identité et les coordonnées d'un point de contact dédié à ces questions.

X. Registre des activités de traitement

Le titulaire déclare **tenir par écrit un registre** de toutes les catégories d'activités de traitement effectuées pour le compte de l'acheteur comprenant :

- Le nom et les coordonnées de l'acheteur 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 de l'acheteur ;
- 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 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.

XI. Documentation

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

XII. Pénalités de retard liées à l'exécution des présentes clauses

La pénalité sera celle appliquée pour « non-respect des consignes de sécurité » indiquée à l'article 5.2 du CCAP.