MINISTÈRE
DE LA JUSTICE
Liberté
Égalité
Fraternité

Direction Générale de
l'administration pénitentiaire

ANNEXE 3 CCAP marché nettoyage

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

1 DESCRIPTION DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL NECESSAIRES A L'EXECUTION DE L'ACCORD-CADRE 2

2 DUREE DE L'ENGAGEMENT DES PARTIES 2

3 OBLIGATIONS DU TITULAIRE 2

3.1 SOUS-TRAITANCE ULTERIEURE 3
3.2 DROIT D'INFORMATION DES PERSONNES CONCERNEES 3
3.3 EXERCICE DES DROITS DES PERSONNES 3
3.4 NOTIFICATION DES VIOLATIONS DES DONNEES A CARACTERE PERSONNEL 3
3.5 AIDE DU TITULAIRE DANS LE CADRE DU RESPECT PAR L'ACHETEUR DE SES OBLIGATIONS 4
3.6 MESURES DE SECURITE DES DONNEES A CARACTERE PERSONNEL 4
3.7 SORT DES DONNEES 4
3.8 DELEGUE A LA PROTECTION DES DONNEES 4
3.9 REGISTRE DES ACTIVITES DE TRAITEMENT 4
3.10 DOCUMENTATION 5

Chaque partie au contrat est tenue au respect des règles relatives à la protection des données à caractère personnel auxquelles elle a accès pour les besoins de l'exécution du contrat. Ces règles sont issues du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 ci-après désigné " le règlement européen sur la protection des données ".

Les dispositions suivantes ont pour objet de définir les conditions dans lesquelles le sous-traitant, au sens du règlement européen sur la protection des données, désigné le titulaire, s'engage à effectuer pour le compte du responsable de traitement, désigné l'acheteur, les opérations de traitement de données à caractère personnel définies ci-après.

1 DESCRIPTION DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL NECESSAIRES A L'EXECUTION DE L'ACCORD-CADRE

Le titulaire est autorisé à traiter pour le compte de l'acheteur les données à caractère personnel nécessaires pour fournir les prestations objet du contrat

2 DUREE DE L'ENGAGEMENT DES PARTIES

Les présentes clauses entrent en vigueur à compter de la notification de l'accord-cadre par l'acheteur au titulaire pour toute la durée d'exécution de l'accord-cadre.

3 OBLIGATIONS DU TITULAIRE

Le titulaire s'engage à :

- traiter les données uniquement pour les seules finalités du traitement,
- traiter les données conformément aux instructions de l'acheteur. Si le titulaire 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 l'acheteur. 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'Etat membre auquel il est soumis, il doit informer 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,
- garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent contrat,
- veiller 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, reçoivent la formation nécessaire en matière de protection des données à caractère personnel, et 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.

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 le bénéficiaire 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 du bénéficiaire.

3.1 Sous-traitance ultérieure.

Le titulaire de l'accord-cadre 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 et le bénéficiaire 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 de l'accord-cadre et les dates du contrat de sous-traitance.
L'acheteur doit recueillir l'avis du bénéficiaire, et dispose d'un délai minium de 15 jours calendaires 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.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions de l'acheteur. Il appartient au titulaire de s'assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en oeuvre 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 demeure pleinement responsable devant l'acheteur de l'exécution par le sous-traitant ultérieur de ses obligations.

3.2 Droit d'information des personnes concernées

Le titulaire, au moment de la collecte des données, doit fournir aux personnes concernées par les opérations de traitement l'information relative aux traitements de données qu'il réalise. La formulation et le format de l'information doivent être convenus avec l'acheteur avant la collecte de données.

3.3 Exercice des droits des personnes

Le titulaire doit aider le bénéficiaire 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).
Lorsque les personnes concernées exercent auprès du titulaire des demandes d'exercice de leurs droits, le titulaire doit adresser ces demandes dès réception par courrier électronique à dbf-uamp.disp-dijon@justice.fr .

3.4 Notification des violations des données à caractère personnel

Le titulaire notifie à l'acheteur toute violation de données à caractère personnel dans un délai maximum de 48 heures après en avoir pris connaissance et par le moyen suivant :

- Par courrier : Ministère de la justice, DPD, 13 Place Vendôme, 75001 Paris
- Par courriel : dpd@justice.gouv.fr

Cette notification est accompagnée de toute documentation utile afin de permettre à l'acheteur, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.
Après accord de l'acheteur, le titulaire notifie à l'autorité de contrôle compétente (la CNIL), au nom et pour le compte de l'acheteur, les violations de données à caractère personnel dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, 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 le 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.

3.5 Aide du titulaire dans le cadre du respect par l'acheteur de ses obligations

Le titulaire aide l'acheteur pour la réalisation d'analyses d'impact relative à la protection des données.
Le titulaire aide l'acheteur pour la réalisation de la consultation préalable de l'autorité de contrôle.

3.6 Mesures de sécurité des données à caractère personnel

Le titulaire s'engage à mettre en oeuvre les mesures de sécurité suivantes :

- 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.

3.7 Sort des données

Au terme de la prestation de services relatifs au traitement de ces données, le titulaire s'engage à 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.

3.8 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 au règlement européen sur la protection des données.

3.9 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 du bénéficiaire comprenant :

- Le nom et les coordonnées du bénéficiaire 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 ;

- 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 les documents attestant de l'existence de garanties appropriées le cas échéant ;

- 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.

3.10 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 le bénéficiaire ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.