ACCORD-CADRE INTERMINISTÉRIEL DE PRESTATIONS DE SERVICES TRAITEURS ET PLATEAUX-REPAS POUR LES SERVICES (HORS MINISTÈRE DES ARMÉES) ET CERTAINS ÉTABLISSEMENTS PUBLICS DE L'ETAT EN RÉGION AUVERGNE-RHÔNE-ALPES

Annexe 3 au CCAP :

Traitement de données à caractère personnel et RGPD

Cas de l'acheteur

Le titulaire de l'accord-cadre est responsable du traitement des données à caractère personnel.

Il fixe les finalités et les moyens du traitement.

Pour l'exécution de l'accord-cadre, en cas de traitement de données à caractère personnel, le titulaire, et le cas échéant ses sous-traitants, est tenu au respect de la réglementation en vigueur applicable au traitement de données à caractère personnel et, notamment 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, et abrogeant la directive 95/46/CE (ci-après, «règlement général sur la protection des données » ou RGPD) et la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Le cas échéant, le titulaire apporte à l'acheteur, avant la mise en application du traitement, des 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 et garantisse la protection des droits des personnes concernées.

Dès la notification de l'accord-cadre, il communique à l'acheteur l'identité et les coordonnées (téléphone et mail) de son délégué à la protection des données (DPD)]

Le présent article a pour objet de définir les conditions dans lesquelles le(s) titulaire(s) du présent accord-cadre s'engage(nt) à effectuer pour le compte de l'acheteur les opérations de traitement de données à caractère personnel définies ci-après.

Dans le cadre du présent accord-cadre, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, notamment le RGPD et la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Précisions terminologiques :

Le responsable de traitement 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 » ou RGPD) est l'acheteur et le sous-traitant est le titulaire du présent accord-cadre.

Nature, durée, finalité et description du traitement de données à caractères personnel

Le titulaire est autorisé à traiter pour le compte de l'acheteur, les données à caractère personnel nécessaires pour fournir les prestations objet de l'accord-cadre.

Les données à caractère personnel sont traitées pour une durée identique à celle de l'accord-cadre.

- **Obligations du titulaire vis-à-vis de l'acheteur**

Le titulaire de l'accord-cadre s'engage, notamment, à :

1. traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet du présent accord-cadre ;

2. Si le titulaire est tenu de procéder à un transfert de données vers un pays tiers (hors de l'Union européenne) 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 ;

Les données transférées vers un pays tiers doivent bénéficier d'un degré de protection équivalent à celui garanti par le RGPD au sein de l'Union européenne. Il est rappelé que tout transfert de données à caractère personnel, au bénéfice de

toute entité et notamment de pays tiers ou d'organisations internationales, qui ne serait pas strictement conforme à la réglementation française ou européenne est formellement prohibé.

A défaut de pouvoir garantir le respect de ces exigences en cas de transfert de données à caractère personnel vers un pays tiers, le titulaire suspend tout transfert et se rapproche de l'acheteur pour envisager, le cas échéant, l'adaptation des modalités d'exécution de l'accord-cadre permettant le respect des exigences du RGPD.

Si les modalités d'exécution ne peuvent être adaptées, l'acheteur procède à la résiliation de l'accord-cadre pour motif d'intérêt général dans les conditions prévues par le CCAG de référence.

Les données transférées vers un pays tiers doivent bénéficier d'un degré de protection équivalent à celui garanti par le RGPD au sein de l'Union européenne. Il est rappelé que tout transfert de données à caractère personnel, au bénéfice de toute entité et notamment de pays tiers ou d'organisations internationales, qui ne serait pas strictement conforme à la réglementation française ou européenne est formellement prohibé.

A défaut de pouvoir garantir le respect de ces exigences en cas de transfert de données à caractère personnel vers un pays tiers, le titulaire suspend tout transfert et se rapproche de l'acheteur pour envisager, le cas échéant, l'adaptation des modalités d'exécution du marché permettant le respect des exigences du RGPD.

Si les modalités d'exécution ne peuvent être adaptées, l'acheteur procède à la résiliation du marché pour motif d'intérêt général dans les conditions prévues par le CCAG de référence.

3. garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent accord-cadre ;

4. veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent accord-cadre :
- 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

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.

- **<u>Sous-traitance des activités de traitement</u>**

Lorsque le titulaire fait appel à un sous-traitant pour mener des activités de traitement spécifiques, il informe préalablement et par écrit l'acheteur. Cette information doit indiquer clairement la nature des activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance. Cette sous-traitance ne peut être effectuée que si l'acheteur n'a pas émis d'objection pendant le délai de 21 jours à compter de la date de réception de la demande en application des dispositions de l'article R.2193-4 du code de la commande publique.

Afin d'obtenir l'acceptation et l'agrément de l'acheteur, le titulaire doit présenter son sous-traitant 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 https://www.economie.gouv.fr/daj/formulaires-declaration-du-candidat).
Le sous-traitant est tenu de respecter les obligations du présent accord-cadre pour le compte et selon les instructions de l'acheteur. Il appartient au titulaire de s'assurer que le sous-traitant 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 de la législation et de la réglementation en vigueur sur la protection des données. Si le sous-traitant 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 de ses obligations. Le titulaire informe préalablement et par écrit l'acheteur de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants

- **Droit d'information et exercice des personnes concernées par le traitement**

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

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

Le titulaire doit répondre, au nom et pour le compte de l'acheteur et dans les délais prévus par le règlement général sur la protection des données, aux demandes des personnes concernées en cas d'exercice de leurs droits.

- **Notification des violations de données à caractère personnel**

Le titulaire notifie à l'acheteur toute violation de données à caractère personnel dans un délai de 24 heures après en avoir pris connaissance et par courriel. 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 (en l'occurrence, à la Commission nationale de l'informatique et des libertés, CNIL) si possible 72 heures au plus tard après en avoir pris connaissance.

Après accord écrit de l'acheteur, le titulaire notifie à l'autorité de contrôle compétente, au nom et pour le compte de l'acheteur, les violations de données à caractère personnel dans un délai maximum de 72 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 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.

Après accord écrit de l'acheteur, le titulaire communique, au nom et pour le compte de l'acheteur, la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et 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 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.

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

Le titulaire aide l'acheteur :

- à la réalisation d'analyses d'impact relative à la protection des données ;
- à la réalisation de la consultation préalable de l'autorité de contrôle.

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

- **Mesures de sécurité**

Le titulaire met 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.

- **Sort des données**

Au terme de l'exécution du présent accord-cadre, l'acheteur informe le titulaire de sa décision relative au sort des données. L'acheteur peut demander au titulaire de :

• détruire toutes les données à caractère personnel
• renvoyer toutes les données à caractère personnel à l'acheteur ou au tiers désigné par l'acheteur

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du sous-traitant. Une fois détruites, le sous-traitant doit justifier par écrit de la destruction.

- **Délégué à la protection des données**

Le titulaire communique à l'acheteur dès la notification de l'accord-cadre le nom

et les coordonnées de son délégué à la protection des données, s'il en a désigné un, ou, à défaut, l'identité et les coordonnées d'un point de contact dédié à ces questions.

- **Registre des activités de traitement**

Le titulaire tient par écrit un registre de toutes les activités de traitement effectuées pour le compte de l'acheteur comprenant :

1. 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 ;

2. les catégories de traitements effectués pour le compte de l'acheteur ;

3. 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 général sur la protection des données, les documents attestant de l'existence de garanties appropriées ;

4. dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, notamment, 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.

Pénalité pour manquement aux obligations associées à la protection des données à caractère personnel :

En cas de méconnaissance de la réglementation liée à la protection des données à caractère personnel et des stipulations du présent document, les pénalités suivantes seront appliquées : 50€ euros pour non transmission du nom et des coordonnées du DPD du titulaire, pour absence de notification à l'acheteur d'une violation de données à caractère personnel, pour non-tenue du registre des activités de traitement ...).

Conformément au CCAG de référence, l'acheteur peut résilier l'accord-cadre pour faute du titulaire en cas de manquement grave et répété, par le titulaire ou son

sous-traitant, aux obligations relatives à la confidentialité, à la protection des données à caractère personnel et à la sécurité prévues par la réglementation française et européenne ainsi qu'aux obligations prévues par le présent article et par les pièces particulières de l'accord-cadre.

Cas des bénéficiaires de l'accord-cadre

- **Sort des données**

Au terme de l'exécution du présent marché public, le bénéficiaire informe le titulaire de sa décision relative au sort des données. Le bénéficiaire peut demander au titulaire de :

• détruire toutes les données à caractère personnel
• renvoyer toutes les données à caractère personnel à l'acheteur ou au tiers désigné par le bénéficiaire

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du sous-traitant. Une fois détruites, le sous-traitant doit justifier par écrit de la destruction.

- **Délégué à la protection des données**

Le titulaire communique au bénéficiaire dès la notification de l'accord-cadre le nom et les coordonnées de son délégué à la protection des données, s'il en a désigné un, ou, à défaut, l'identité et les coordonnées d'un point de contact dédié à ces questions.

- **Registre des activités de traitement**

Le titulaire tient par écrit un registre de toutes les activités de traitement effectuées pour le compte du bénéficiaire comprenant :
1. 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 ;
2. les catégories de traitements effectués pour le compte de l'acheteur ;
3. 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 général sur la protection des données, les documents attestant de l'existence de garanties appropriées ;
4. dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, notamment, 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.

Pénalité pour manquement aux obligations associées à la protection des données à caractère personnel :

En cas de méconnaissance de la règlementation liée à la protection des données à caractère personnel et des stipulations du présent document, les pénalités suivantes seront appliquées :
- 50 euros par jour de retard (à compter du jour de la notification) en cas de non-communication de l'identité du DPD,
- 50 euros par heure de retard en cas de non-respect du délai de notification des violations de données à caractère personnel...

Conformément au CCAG de référence, le bénéficiaire peut résilier l'accord-cadre pour faute du titulaire en cas de manquement grave et répété, par le titulaire ou son sous-traitant, aux obligations relatives à la confidentialité, à la protection des données à caractère personnel et à la sécurité prévues par la réglementation française et européenne ainsi qu'aux obligations prévues par le présent article et par les pièces particulières de l'accord-cadre.

Confidentialité et secret des affaires

Le titulaire s'engage à mettre en oeuvre les moyens appropriés afin de garder confidentiels les informations, les documents et les objets auxquels il aura eu accès lors de l'exécution de l'accord-cadre, sans qu'il soit besoin d'en expliciter systématiquement le caractère confidentiel. Ces informations, documents ou objets ne peuvent être, sans autorisation expresse de l'acheteur, divulgués, publiés, communiqués à des tiers ou être utilisés directement par le titulaire, hors de l'accord-cadre ou à l'issue de son exécution.

Le titulaire s'engage à faire respecter ces obligations à l'ensemble de son personnel, le cas échéant à ses sous-traitants et fournisseurs. L'acheteur peut demander, à tout moment, au titulaire, de lui retourner les éléments ou supports d'informations confidentielles qui lui auraient été fournis, sans en conserver aucune copie ou trace. La violation de l'obligation de confidentialité par le titulaire pourra entraîner la résiliation de l'accord-cadre aux torts du titulaire.

Le titulaire ne peut divulguer les données et informations couvertes par le secret des affaires dont il aurait connaissance pendant la durée d'exécution de l'accord-

cadre. Dans l'hypothèse où il aurait connaissance de telles informations, il s'engage à mettre en oeuvre l'ensemble des moyens nécessaires afin de réduire les risques de divulgation, notamment au moyen d'engagements de confidentialité individuels, de cloisonnement organisationnel et de paramétrage des droits d'accès. En cas de violation de cette obligation, le titulaire encourt une pénalité forfaitaire d'un montant de 100€ par document divulgué en méconnaissance du secret des affaires, ainsi que, en cas de manquement grave ou répété, la résiliation de l'accord-cadre à ses torts. Cette interdiction ne prend pas fin à l'issue de l'accord-cadre.

Le titulaire consent, en application de l'article L. 151-5 du code de commerce, à ce que tous les documents
de son offre et ceux liés à l'exécution de l'accord-cadre puissent être divulgués par l'acheteur à un tiers, à la condition que cette divulgation s'avère nécessaire, notamment pour les besoins d'une mission de conseil ou
d'assistance à maîtrise d'ouvrage, de contrôle des prestations réalisées ou en cas de passation d'un accord-cadre de substitution.

L'acheteur s'engage, le cas échéant, à obtenir de ce tiers toutes les assurances nécessaires quant à la mise
en oeuvre par ce dernier et ses éventuels sous-traitants de mesures effectives de protection des informations couvertes par le secret des affaires.

L'acheteur informe le titulaire par écrit 15 jours avant de divulguer de telles informations, en précisant le motif, la durée ainsi que les informations et documents concernés.
Tout au long de l'exécution de l'accord-cadre, le titulaire est tenu de déclarer sans délai à l'acheteur toute situation de nature à constituer un conflit d'intérêts.