DNID-2026-EXPERTISE-BIJOUTERIE

ANNEXE au CCAP

OBLIGATIONS RELATIVES A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

CLAUSE n°1 - **DEFINITIONS REGLEMENTAIRES**

« Données à caractère personnel » : Toute information se rapportant à une personne physique identifiée ou identifiable directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

« Traitement » : Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

« Personne publique » : Responsable de traitement consacré par la réglementation nationale et européenne relative à la protection des données à caractère personnel, c'est-à-dire la personne morale, l'autorité publique, le service ou tout autre organisme de la Direction générale des finances publiques (DGFIP) qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens d'un traitement et décide d'en collecter les données à caractère personnel.

« Responsable du traitement » : Personne physique ou morale, autorité publique, service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre. En spécifiant et en achetant les Services, la personne publique revêt la qualité de Responsable de Traitement

« Titulaire » : Personne physique ou morale, le service ou tout autre organisme distinct de la personne publique qui accède et traite des données à caractère personnel pour le compte de cette dernière sans avoir eu l'initiative de leur collecte. Il correspond également au sous-traitant tel qu'identifié par la réglementation nationale et européenne relative à la protection des données à caractère personnel.

« Sous-traitant » : Prestataire agréé par la personne publique pour exécuter une partie des prestations du marché dans le cadre d'un contrat de sous-traitance signé avec le titulaire du marché public. Ce prestataire est un sous-traitant direct (de niveau 1) ou un sous-traitant indirect (de niveau 2 et de niveaux inférieurs) du titulaire. Il correspond également au sous-traitant tel que le consacre la réglementation nationale et européenne relative à la protection des données à caractère personnel.

« Personne concernée » : Personne physique dont les données à caractère personnel font l'objet d'un traitement dans le cadre des prestations du marché.

« Réglementation nationale et européenne sur la protection des données à caractère personnel » : Ensemble des textes juridiques français (loi n°78-17 du 6 janvier 1978 modifiée) et européens (Règlement 2016/679/UE et Directive 2016/680/UE des 27 avril 2016) fixant les conditions d'utilisation des données à caractère personnel lorsque des traitements automatisés sont mis en œuvre pour exécuter les prestations du marché.

« Pseudonymisation » Traitement qui garantit que des données à caractère personnel ne pourront plus être attribuées à une personne physique précise sans avoir recours à des informations supplémentaires conservées séparément et soumises à des mesures techniques et organisationnelles.

Violation de données à caractère personnel » : 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 transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

« Mesures techniques et organisationnelles » : Mesures destinées à protéger les données à caractère personnel contrer une destruction fortuite ou illicite, une perte fortuite, une altération, une divulgation ou un accès non autorisé, notamment lorsque le traitement suppose la transmission de données par réseau, et contre toute forme illicite de traitement.

CLAUSE n°2 - **POLITIQUE DE CONFORMITE AU RGPD**

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

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 dénommé le « RGPD »).

Les Parties s'engagent également à respecter toute évolution de la législation ou de la réglementation française ou européenne qui impacterait en ce domaine les conditions d'exécution du marché.

CLAUSE n°3 - **DESCRIPTION DES TRAITEMENTS FAISANT L'OBJET DES PRESTATIONS**

Le titulaire est autorisé à traiter pour le compte de la personne publique les données à caractère personnel nécessaires pour fournir les services prévus par les prestations du marché.

Le traitement mis en œuvre au titre du présent marché répond aux caractéristiques suivantes :

- Les opérations réalisées sur les données sont l'expertise de biens dont les services de l'État n'ont plus l'utilité, les biens issus de scellés de justice, objets trouvés remis par les communes, biens dépendant de successions vacantes, biens abandonnés en établissement de santé, objets trouvés,

- La(les) finalité(s) du traitement sont la vente des biens pour le compte des services ayant remis les biens au Domaine,

- Les catégories de données à caractère personnel traitées sont les identifiants du système d'information VEGA,

- Les catégories de personnes concernées sont des personnes physiques, morales.

CLAUSE n°4 - **CONDITIONS DE TRAITEMENT DES DONNEES A CARACTERE PERSONNEL**

Le titulaire s'engage à :

1. traiter les données uniquement pour la ou les seule(s) finalité(s) qui font l'objet du présent marché ;

2. traiter les données conformément aux instructions documentées de la personne publique;

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

4. veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent marché s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité et 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 ainsi que le prévoit la Directive 2014/24/UE du 26 février 2014 sur la passation des marchés publics (considérant 77) ;

6. édicter à son personnel des directives relatives à la mise en œuvre des mesures prévues par la réglementation nationale et européenne relative à la protection des données à caractère personnel et à la démonstration du respect de cette dernière. L'application par le titulaire de codes de conduite ou de mécanisme de certification approuvés, voire d'indications données par un délégué à la protection des données peut servir à démontrer le respect des obligations incombant à la personne publique.

Au terme de la prestation de services relatifs au traitement des données à caractère personnel, le titulaire s'engage au choix de la personne publique qui sera spécifié par écrit le moment venu à (i) détruire toutes les données à caractère personnel ou (ii) à les lui renvoyer ou (iii) à les renvoyer à ses sous-traitants. Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du titulaire et des sous-traitants. Le titulaire et ses sous-traitants justifient par écrit de la destruction.

CLAUSE n°5 - **OBLIGATIONS DU TITULAIRE A L'EGARD DES SOUS-TRAITANTS**

Le titulaire s'engage à respecter et à faire respecter par l'ensemble des sous-traitants directs et indirects du marché ainsi qu'à leurs personnels respectifs les mêmes obligations en matière de protection de données à caractère personnel que celles fixées dans le présent marché, en particulier pour ce qui est de présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées.

Pour ce faire, le titulaire s'engage à insérer et à faire insérer dans les différents contrats de sous-traitance les clauses de protection des données à caractère personnel adoptées par la Commission européenne et/ou par la CNIL.

Si les sous-traitants ne remplissent pas leurs obligations en matière de protection des données, le titulaire demeure pleinement responsable devant le responsable de traitement de l'exécution de ses obligations par ces derniers. Le titulaire est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour fournir les prestations définies par le présent marché.

CLAUSE n°6 - **OBLIGATIONS DE LA PERSONNE PUBLIQUE A L'EGARD DU TITULAIRE**

La personne publique s'engage à :

- 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 règlement européen sur la protection des données de la part du titulaire ;

- superviser le traitement, y compris réaliser les audits et les inspections auprès du titulaire.

CLAUSE n°7 - **REGISTRE ET DOCUMENTATION DES TRAITEMENTS**

Registre des catégories d'activités de traitement

Le titulaire s'engage à tenir un registre de toutes les catégories d'activités de traitement effectuées pour le compte de la personne publique en vue d'une mise à disposition de la CNIL sur demande de celle-ci.

Le registre se présente sous une forme écrite y compris électronique et comprend :
- le nom et les coordonnées de la personne publique pour le compte duquel il agit, du titulaire et des éventuels sous-traitants ;
- les noms et les coordonnées du délégué à la protection des données du titulaire ;
- les catégories de traitements effectués pour le compte de la personne publique ;
- si possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins (i) la pseudonymisation et le chiffrement des données à caractère personnel, (ii) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement, (iii) 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, (iv) 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 RGPD, les documents attestant de l'existence de garanties appropriées.

Documentation

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

CLAUSE n°8 - **SECURITE DES DONNEES A CARACTERE PERSONNEL**

Le titulaire exécute, sous le contrôle de la personne publique, les prestations du marché en mettant en œuvre les mesures techniques et organisationnelles appropriées et en garantissant aux données à caractère personnel un niveau de sécurité adapté aux risques, compte tenu de l'état des connaissances disponibles et des coûts induits par le traitement des données.

Les mesures mises en œuvre à ce titre privilégient notamment (i) les techniques de pseudonymisation et de chiffrement des données à caractère personnel, (ii) les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement, (iii) 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 puis (iv) les mesures de sécurité prévues par ses codes de conduite, interne et/ou par toute certification si le titulaire en dispose.

Il met en œuvre une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement des données à caractère personnel.

Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite qui sont susceptibles d'entraîner des dommages physiques, matériels ou un préjudice moral. La personne publique et le titulaire prennent des mesures afin de garantir que toute personne physique qui, pour l'exécution des prestations, accède à des données à caractère personnel, agit bien sous l'autorité de l'un d'entre eux.

Le titulaire s'engage à utiliser et à faire utiliser par les sous-traitants des moyens conformes à la politique générale de sécurité des systèmes d'information de l'État (circulaire du Premier ministre du 17 juillet 2014) et des ministères économiques et financiers (Arrêté du 1er août 2016), pour (i) garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes d'information, (ii) rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais adaptés en cas d'incident physique ou technique.

Conformément à la réglementation nationale et européenne relative à la protection des données à caractère personnel, le titulaire s'engage à préserver et à faire préserver par les sous-traitants la sécurité des informations et des données qui lui sont confiées en prenant toute mesure adaptée. Ces mesures visent à empêcher que les données à caractère personnel soient déformées, endommagées, ou que des tiers non autorisés y aient accès. Le titulaire informera son personnel et sensibilisera les sous-traitants qui pourraient intervenir pour son compte sur les obligations de sécurité informatique mises à leur charge.

Prestations en environnement IPV6

Le titulaire et les sous-traitants sont informés que la réalisation des prestations dans un environnement naissant IPV6 voire dans un environnement passerelle de transition IPv4/IPv6 est de nature à réduire la sécurité informatique du patrimoine logiciel et matériel de la personne publique :
- impacts sur les données et les traitements de la DGFIP exploités pour son compte ;
- impacts sur les flux informatiques échangés avec les partenaires de la personne publique ;
- impacts sur le dimensionnement des services support (maintenance, profils métier notamment).

A ce titre, chaque partie prend les mesures nécessaires et les précautions utiles pour renforcer la sécurité informatique des prestations et garantir la protection des données à caractère personnel au regard (i) de la nature des données et des risques soulevés par leur traitement, (ii) des contraintes réglementaires imposant la prise en compte de normes techniques spécifiques.

Prestations adossées à des solutions de type cloud

Dans l'hypothèse où les prestations seraient exécutées au moyen de solutions en nuage (de type « cloud ») nécessaires à l'exercice des missions confiées, le titulaire s'engage à héberger et à faire héberger les données de production mises à disposition par la personne publique en un lieu géographique relevant d'une législation qui assure un niveau de protection des données à caractère personnel au moins équivalent à celui assuré par la réglementation nationale et européenne.

CLAUSE n°9 – **DEVOIR D'INFORMATION ET DEVOIR D'ALERTE**

Le titulaire s'engage à signaler et à faire signaler à la personne publique dans un délai inférieur à 5 jours calendaires tous les éléments qui lui paraîtraient de nature à compromettre la bonne exécution du marché.

Sécurité informatique

Le titulaire s'engage à informer le responsable de traitement et à être informé par ses sous-traitants de (i) tout incident de sécurité concernant les moyens informatiques utilisés au titre du marché (intrusion logique, altération malveillante, dégradation volontaire, infection par virus informatique, disparition de supports exploités sur les lieux d'exécution des prestations), (ii) tout événement affectant ou susceptible d'affecter la sécurité ou le fonctionnement des systèmes d'information d'importance vitale de la personne publique au sens des articles L. 1332-6-2 et R. 1332-41-10 du code de la défense nationale dès lors que ceux-ci sont concernés par l'exécution des prestations, (iii) toute évolution qui affecterait les conditions de traitement et d'exploitation des données à caractère personnel envisagées pour exécuter les prestations du marché.

A titre indicatif, sont concernés (i) les solutions de virtualisation de traitements lorsque les fonctionnalités mises en œuvre permettent de transférer des données entre des serveurs physiques implantés dans des pays dont l'un d'eux relève d'une réglementation qui ne garantit pas un niveau de protection des données à caractère personnel adéquat ou équivalent à celui prévu par la réglementation européenne (cas des migrations à chaud de machines virtuelles notamment), (ii) les déménagements de serveurs hébergeant des traitements et des données accédées et/ou exploitées pour le compte de la personne publique, (iii) les moyens d'accès et de transfert de données à caractère personnel (solutions d'authentification, protocoles d'échanges de données notamment).

Dans tous les cas, le titulaire vérifie et s'engage à faire vérifier par ses sous-traitants que l'environnement et les conditions d'exploitation des données à caractère personnel respectent les standards et les normes de sécurité informatiques validés par l'Agence nationale pour la sécurité des systèmes d'information (ANSSI) et repris dans la politique générale de sécurité des systèmes d'information de l'État (circulaire du Premier ministre du 17 juillet 2014) et des ministères économiques et financiers (Arrêté du 1er août 2016).

Instruction contraire à la réglementation

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 le responsable de traitement.

Transfert de données vers un pays tiers

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 en informe le responsable du traitement au préalable , sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

Tout manquement constaté à ces obligations constitue une faute du titulaire.

CLAUSE n°10 – **NOTIFICATION DES VIOLATIONS DE DONNEES A CARACTERE PERSONNEL**

Notification des violations à la personne publique

Le titulaire s'engage à notifier dans un délai de 48 heures à la personne publique toute violation de données à caractère personnel en rapport avec l'exécution des prestations après en avoir pris connaissance, dès lors que ces dernières ne sont couvertes par aucun procédé d'anonymisation irréversible.

Cette 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.

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.

Notification des violations aux personnes concernées

Après accord du responsable de traitement, le titulaire communique, au nom et pour le compte du responsable de traitement, 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 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.

Tout manquement constaté à ces obligations constitue une faute du titulaire et/ou de ses sous-traitants.

CLAUSE n°11 – **DEVOIR DE COOPERATION**

Le titulaire et la personne publique s'engagent à une coopération réciproque et loyale pour la bonne exécution des prestations et le traitement licite des données à caractère personnel qui en découle.

Désignation d'un Délégué à la Protection des Données

Le titulaire s'engage à désigner et à faire désigner par ses sous-traitants chacun pour ce qui les concerne un délégué à la protection des données (DPD).
Il en communique le nom et les coordonnées à la personne publique.
Le titulaire veille à ce que le DPD soit associé en temps utile, à toutes les questions relatives à la protection des données à caractère personnel que soulèverait l'exécution des prestations.

Audits des traitements par la personne publique

La personne publique se réserve la possibilité de tester, analyser et évaluer régulièrement, les mesures techniques, organisationnelles et de mise en conformité des process métiers afin de vérifier leur efficacité. Ces vérifications peuvent prendre la forme d'un audit sur place ou sur pièce.
Le titulaire s'engage à permettre la réalisation des audits décidés par la personne publique et d'y contribuer à ces audits. Il s'engage également à permettre le déroulement des contrôles que la CNIL pourrait effectuer sur place ou sur pièces sur les traitements de données à caractère personnel mis en œuvre dans le cadre des prestations du marché.

Mise à disposition des informations requises par les institutions publiques

Sur demande de la personne publique, le titulaire lui communique toute précision (i) garantissant à la CNIL la régularité des traitements automatisés de données à caractère personnel utilisés ou élaborés pour les besoins du marché et (ii) permettant de répondre aux questions parlementaires (éléments statistiques et volumétriques volumétrie de certaines catégories d'informations portant sur des données traitées dans les applications de la DGFIP notamment).

Intervention au titre des installations d'importance vitale de la personne publique

Sur demande de la personne publique, le titulaire l'assiste dans le cadre des procédures d'audit et de contrôle susceptibles d'être déployées dans les sites classés « points d'importance vitale » notamment.
Il apporte, à ce titre, et en tant que de besoin, toute information permettant à la personne publique, aux experts et aux membres de la commission de défense et de sécurité de vérifier et de constater que les mesures de protection mises en oeuvre dans les installations d'importance vitale notamment, et applicables aux prestations de l'accord-cadre, ne contiennent pas de failles de sécurité évidentes.

Assistance demandée par la personne publique

Dans la limite des informations disponibles, le titulaire s'engage à assister la personne publique à sa demande et à obtenir de ses sous-traitants une assistance identique dans les cas suivants :
- donner suite, dans les délais requis, aux demandes et actions exercées à son encontre par les personnes concernées au titre de la réglementation relative à la protection des données à caractère personnel ;
- réaliser l'analyse d'impact relative à la protection des données et la consultation préalable de la CNIL
- honorer son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement, d'opposition et de limitation du traitement.

CLAUSE n°12 - **SANCTIONS**

Tout manquement constaté et dûment établi aux obligations prévues par le présent marché pour protéger les données à caractère personnel, expose le titulaire à la résiliation du marché à ses frais et risques conformément aux articles 42 et 46 du CCAG.

En cas de non-respect de l'obligation de sécurité informatique prévue au marché, la responsabilité du titulaire peut être engagée sur la base de l'article 226-17 du code pénal.