

**ANNEXE NUMÉRO 2**

**OBLIGATIONS RELATIVES A LA PROTECTION  
DES DONNÉES A CARACTÈRE PERSONNEL DANS LE CADRE DE LA  
SOUS-TRAITANCE ULTÉRIEURE**

## CLAUSE n°1 - DEFINITIONS REGLEMENTAIRES

**1.1. « 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.

**1.2. « Données à caractère non personnel » :** Données qui ne sont pas des données à caractère personnel au sens du RGPD à savoir d'une part, les données qui, au départ, ne concernaient pas une personne physique identifiée ou identifiable et d'autre part, les données qui étaient initialement des données à caractère personnel, mais qui ont ensuite été rendues anonymes.

**1.3. « Données mixtes » :** Tout ensemble de données mixte comportant à la fois des données à caractère personnel et des données à caractère non personnel.

**1.4. « 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.

**1.5. « 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 personnelles.

**1.6. « 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 d'un État membre. En spécifiant et en achetant les Services, la personne publique revêt la qualité de Responsable de Traitement

**1.7. « 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.

**1.8. « 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 au sous-traitant consacré par la réglementation relative à la protection des données à caractère personnel.

**1.9. « Personne concernée » :** Personne physique dont les données personnelles font l'objet d'un traitement dans le cadre des prestations du marc

**hé.1.10. « Réglementation nationale et européenne sur la protection des données à caractère personnel » :** Loi n°78-17 du 6 janvier 1978 modifiée, Règlement 2016/679/UE et Directive 2016/680/UE des 27 avril 2016 fixant les conditions d'utilisation des données à caractère personnel.

**1.11. « 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.

**1.12. « 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 personnelles transmises, conservées ou traitées ou l'accès non autorisé à de telles données.

**1.13. « Mesures techniques et organisationnelles »** : Mesures destinées à protéger les données personnelles contre 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**

2.1. 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.

2.2. 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 »).

2.3. Les parties s'engagent également à respecter la réglementation en vigueur applicable au traitement de données mixtes et, en particulier, le Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne applicable depuis le 18 juin 2019 et les lignes directrices de la Commission européenne du 29 mai 2019 relatives au règlement applicable au libre flux des données à caractère non personnel dans l'Union européenne.

2.4. Lorsque les échanges intervenus dans le cadre du présent marché sont constitués d'un ensemble composite intégrant à la fois des données à caractère personnel et des données à caractère non personnel, le niveau de protection mis en œuvre doit tenir compte des prescriptions prévues par l'article 2.2 du Règlement 2018/1807 et par l'article 2.2 des lignes directrices de la Commission européenne du 29 mai 2019. En pareille situation, les conditions et les modalités d'utilisation des données à caractère non personnel et des données à caractère personnel de l'ensemble sont respectivement définies par le Règlement (UE) 2018/1807 pour les premières et par le Règlement (UE) 2016/679 pour les secondes. Lorsque les données à caractère non personnel et les données à caractère personnel sont inextricablement liées, les droits et obligations en matière de protection des données découlant du RGPD s'appliquent pleinement à l'intégralité de l'ensemble de données mixtes, même lorsque les données à caractère personnel ne représentent qu'une petite partie de l'ensemble de données.

2.5. 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

3.1. Le Titulaire et ses Sous-traitants sont autorisés 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. Les opérations réalisées sur demande de la Personne publique par le Titulaire et ses Sous-traitants ont vocation à conférer à ces derniers un accès aux données à caractère personnel issu du traitement Portail Commun de Recouvrement (PCR) ainsi que de la Vue agent lié au portail précité.

3.2. Ces opérations sont les suivantes :

- la pseudonymisation des données réelles pour la réalisation des phases de test ;
- la réalisation de test sur les données réelles en phase de pré-production.

3.3. Elles sont réalisées en exécution des prestations suivantes prévues par le marché :

- développement, la réalisation de tests et de l'architecture applicative dans le cadre de l'assistance à la maîtrise d'œuvre pour la réalisation de projets en environnement ouvert.

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

3.4.1. Les finalités du traitement sont :

- la mise à disposition des usagers professionnels d'un espace de consultation unique des informations liées au recouvrement des créances fiscales et sociales publiques de l'entreprise incluant la création d'un compte sur cet espace, la gestion de ce dernier et des habilitations y afférentes ;
- le rattachement des comptes tiers détenus par l'utilisateur professionnel au compte qu'il possède sur le portail commun de recouvrement incluant la transmission de données au profit des entités tierces assurant la gestion de ces comptes et qui fournissent les données liées au recouvrement des créances fiscales et sociales publiques de la personne morale à laquelle est rattaché l'utilisateur professionnel ;
- la simplification de la création des comptes tiers au profit des entités tierces fournissant les données liées au recouvrement des créances fiscales et sociales publiques de la personne morale à laquelle est rattachée l'utilisateur professionnel ;
- la gestion des abonnements à la newsletter du portail ;
- la mesure d'audience du portail commun de recouvrement ainsi que de la vue agent ;
- mise à disposition d'un espace de consultation des informations fiscales, douanières et sociales des personnes morales redevables de créances publiques dans les domaines précités pour les agents habilités dans le cadre de leurs missions rattachés à la Direction Générale des Finances Publiques, la Direction des Douanes et des Droits Indirects et à la Caisse Nationale de l'Union de Recouvrement des cotisations de Sécurité Sociale et d'allocations familiales (Agence centrale des organismes de sécurité sociale) à des fins de gestion de leurs dossiers.

3.4.2. Les catégories de données à caractère personnel traitées sont :

\* Des données relatives à l'identification des personnes morales telles que les numéros SIREN, numéro SIRET, numéro ITIP, la raison sociale, la forme juridique, etc. ;

\* Des données relatives à l'identification des personnes physiques telles que la civilité, le nom, le prénom, l'adresse électronique professionnelle, le numéro de téléphone portable et le cas échéant, le numéro de téléphone fixe ainsi que l'identifiant PCR de l'utilisateur professionnel et les identifiants sous lesquels ce dernier est connu dans les systèmes d'information des entités tierces qui fournissent les données liées au recouvrement des créances fiscales et sociales publiques de la personne morale à laquelle est rattaché ledit usager, l'identifiant des agents habilités à consulter les informations depuis la vue agent du portail, etc. ;

\* Des données relatives à la vie professionnelle des personnes physiques telles que la qualité de dirigeant et le cas échéant le numéro de demande ProConnect, les habilitations détenues par l'utilisateur professionnel sur le compte tiers des entités tierces fournissant les données liées au recouvrement des créances fiscales

et sociales publiques de la personne morale à laquelle est rattaché l'utilisateur, les rôles détenus par l'utilisateur professionnel sur le compte PCR, l'historique des demandes de rôle traitées par l'utilisateur professionnel, l'historique des rattachements de compte opérés par celui-ci, etc. ;

\* Des informations d'ordre économique et financier telles que les créances fiscales, douanières et sociales publiques dont est titulaire la personne morale concernée, les impositions/droits auxquels est soumise la personne morale concernée, l'identifiant des obligations fiscales auxquelles la personne morale concernée est soumise, les dates des déclarations liées aux impositions/droits auxquels est soumise la personne morale concernée, l'historique des déclarations, l'historique des paiements liés à ces créances, l'échéancier des paiements en cours, le calendrier des futurs paiements, le moyen de paiement utilisé, les mandats bancaires, les demandes de remboursement sollicitées par la personne morale, etc. ;

\* Des données de connexion telles que l'identifiant des personnes physiques/personnes morales, les action(s), date et heure, etc. ;

\* D'autres données liées aux démarches en ligne telles que l'historique des démarches en ligne effectuées depuis le portail par l'utilisateur professionnel, le statut et suivi desdites démarches, les demandes d'assistance formulées par l'utilisateur professionnel ainsi que des données relatives aux statistiques d'audience et d'utilisation des services du portail et de la vue agent.

3.4.3. Les catégories de personnes concernées sont les suivantes : l'utilisateur professionnel et les agents habilités de la Direction Générale des Finances Publiques, la Direction des Douanes et des Droits Indirects et l'Urssaf Caisse Nationale.

3.5. La durée des opérations de traitement précitées réalisées sur les données à caractère personnel par le Titulaire et ses éventuels Sous-traitants s'étend jusqu'au terme du marché, le cas échéant sa dénonciation, sans préjudice d'un éventuel renouvellement de ce dernier.

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

### 4.1. Le Titulaire s'engage à :

- traiter les données uniquement pour la ou les seule(s) finalité(s) qui font l'objet du présent marché ;
- traiter les données conformément aux instructions documentées de la Personne publique;
- garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent marché ;
- 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 ;
- 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 ;
- 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.

### 4.2. Lieu du traitement et transfert de données à caractère personnel

4.2.1. Le Titulaire garantit, pendant toute la durée des prestations, que l'intégralité des données à caractère personnel sont, en exécution de la présente convention, traitées et plus généralement rendues accessibles exclusivement au sein :

- de l'Espace économique européen ;
- ou d'un État tiers bénéficiant d'une décision d'adéquation au sens de l'article 45 du RGPD.

4.2.2. A défaut, en cas de transferts résultant de la réalisation des prestations, le Sous-traitant s'engage à mettre en oeuvre les garanties appropriées ou des règles d'entreprise contraignantes au sens des articles 46 et 47 du RGPD, le cas échéant complétées par des mesures supplémentaires visant à garantir qu'il ne pourra pas y être fait échec dans l'État tiers de destination, dans le strict respect de la jurisprudence.

4.2.3. Les garanties apportées par le sous-traitant sur ce point doivent non seulement couvrir l'hébergement des données, mais également toutes les opérations de traitement réalisées par le Sous-traitant ou par les Sous-traitants ultérieurs auxquels pourraient le cas échéant être confiées certaines opérations de traitement (telles que la maintenance, l'assistance...).

4.2.4 Le Sous-traitant doit ainsi pouvoir garantir que les données traitées ne peuvent pas être rendues accessibles à des destinataires, y compris des autorités administratives ou judiciaires, situés hors de l'Espace économique européen sans que soit respecté le droit applicable, et en particulier le RGPD. Le sous-traitant détaillera les moyens mis en place pour y répondre.

4.2.5. Préalablement à tout transfert, le Titulaire en informe le Responsable de traitement dans un délai raisonnable.

### 4.3 Destruction ou renvoi des données à caractère personnel

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. 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**

5.1. Le Titulaire peut faire appel à un ou plusieurs Sous-traitants pour mener des activités de traitement spécifiques.

5.2. Le Titulaire s'engage à ne pas recruter un autre Sous-traitant sans l'autorisation écrite préalable, spécifique ou générale, du Responsable du traitement. Dans le cas d'une autorisation écrite générale, le Titulaire informe préalablement et par écrit la Personne publique de tout changement envisagé concernant l'ajout ou le remplacement de Sous-traitants ultérieurs. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du Sous-traitant et les dates du marché public. 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.

5.3. 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.

5.4. 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 :

- fournir au Titulaire les données visées à la clause n°3 des présentes ;
- 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.

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

### 7.1. Registre des catégories d'activités de traitement

7.1.1. 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.

7.1.2. 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.

### 7.2. 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

8.1. 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.

8.2. 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.

8.3. 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.

8.4. 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.

8.5. 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.

8.6. 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.

### 8.7. Prestations en environnement IPV6

8.7.1. 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).

8.7.2. 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.

### 8.8. 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.

En outre, si le prestataire offrant la solution en nuage est soumis à la législation d'un pays tiers ne permettant pas d'assurer un niveau de protection approprié des données personnelles au regard du RGPD, notamment en ce qui concerne un éventuel accès des autorités publiques de ce pays tiers aux données, le Titulaire s'engage :

- à signer, s'il est le prestataire, ou à faire signer au sous-traitant-ultérieur prestataire, les clauses contractuelles types 2021/914 de la Commission européenne ;

- à informer la Personne publique de tout recours à une solution en nuage préalablement à l'exécution des prestations correspondantes. À cette occasion le Titulaire communique à la Personne publique les mesures techniques et organisationnelles supplémentaires qu'il s'engage à mettre en œuvre pour établir un niveau de protection suffisant, en assurant a minima la mise en place d'une procédure de chiffrement garantissant la maîtrise de la gestion des clés par le Responsable de traitement afin d'empêcher la lecture des données par des tiers.

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

9.1. Le Titulaire s'engage à signaler et à faire signaler à la Personne publique dans un délai inférieur à 5 (cinq) jours calendaires tous les éléments qui lui paraîtraient de nature à compromettre la bonne exécution du marché.

### 9.2. Sécurité informatique

9.2.1. 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.

9.2.2. 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).

9.2.3. 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).

### 9.3. 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.

### 9.4. Transfert de données vers un pays tiers

9.4.1. 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 sous-traitant suspend tout transfert et informe le Responsable de traitement en vue d'envisager, le cas échéant, l'adaptation des modalités d'exécution de la convention permettant le respect des exigences du RGPD.

9.4.2. Préalablement à tout transfert vers un pays tiers ou vers une organisation internationale situé(e) en dehors du territoire de l'Union européenne et/ou en dehors de l'Espace Economique Européen dans les cas énumérés au point 4.2, le sous-traitant en informe le Responsable de traitement dans un délai raisonnable.

9.5. Tout manquement constaté à ces obligations constitue une faute du Titulaire.

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

### 10.1. Notification des violations à la Personne publique

10.1.1. Le Titulaire s'engage à notifier dans un délai de 48 (quarante-huit) heures à la Personne publique toute violation de données à caractère personnel en rapport avec l'exécution des prestations après en avoir pris connaissance.

10.1.2. 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

10.1.3. 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.

### 10.2. Notification des violations aux personnes concernées

10.2.1. Le Responsable de traitement communique 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. Le Titulaire lui apporte son assistance sur cette communication à la demande du responsable de traitement et compte tenu de la nature du traitement, des informations à la disposition du Titulaire et des compétences du Titulaire.

10.2.2. 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.

10.3. Tout manquement constaté à ces obligations constitue une faute du Titulaire et/ou de ses Sous-traitants.

## CLAUSE n°11 – DEVOIR DE COOPERATION

11.1. 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.

### 11.2. Désignation d'un Délégué à la Protection des Données

11.2.1. 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).

11.2.2. Il en communique le nom et les coordonnées à la personne publique ainsi que toute modification afférente.

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.

### 11.3. Audits des traitements par la Personne publique

11.3.1. 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.

11.3.2. Le Titulaire s'engage à permettre la réalisation des audits décidés par la personne publique et d'y contribuer. Il s'engage à permettre le déroulement des contrôles que la CNIL pourrait effectuer sur place ou sur pièces sur les traitements de données personnelles mis en œuvre pour les prestations du marché.

### 11.4. 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 personnelles 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).

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

11.5.1. 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.

11.5.2. 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 œuvre dans les installations d'importance vitale notamment, et applicables aux prestations de l'accord-cadre, ne contiennent pas de failles de sécurité évidentes.

### 11.6. 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 (i) 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, (ii) réaliser l'analyse d'impact relative à la protection des données et la consultation préalable de la CNIL, (iii) honorer son obligation de donner suite aux demandes d'exercice des droits des personnes concernées (droits d'accès, de rectification, d'effacement, d'opposition et de limitation du traitement).

## CLAUSE n°12- **RESPONSABILITÉ**

12.1. Conformément aux dispositions de l'article 82 du RGPD toute personne physique ayant subi un dommage matériel ou moral du fait d'une violation de la réglementation en matière de protection des données à caractère personnel notamment le RGPD et la LIL, a le droit d'obtenir du Responsable du traitement ou du Sous-traitant réparation du préjudice subi. Il est convenu que le Responsable de traitement ou le Sous-traitant et le cas échéant ses sous-traitants ultérieurs sont tenus responsables du dommage subi par la personne physique concernée à hauteur respective de leur part de responsabilité dans celui-ci.

12.2. Le Responsable de traitement, le Sous-traitant et le cas échéant, ses Sous-traitants ultérieurs sont exonérés de responsabilité s'ils prouvent que le fait qui a provoqué le dommage qu'a subi la ou les personnes physiques concernées par le traitement, ne leur est nullement imputable.



### CLAUSE n°13 - **SANCTIONS**

13.1. 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.

13.2. 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.