



**PRÉFET
DE LA ZONE
DE DÉFENSE
ET DE SÉCURITÉ
OUEST**

*Liberté
Égalité
Fraternité*

Préfecture de zone SGAMI Ouest

Marché public de travaux

Passé en application de la procédure avec négociation et organisation d'un jury (articles L2124-1, L2124-3, R2124-1, R2124-3, R2161-12 à R2161-20 et R2171-16 du code de la commande publique)

***Marché public global sectoriel de conception, construction,
aménagement, entretien, hôtellerie et de maintenance pour une
opération comprenant la création d'un Centre de Rétention
Administrative (CRA) et d'une Annexe de Justice à Oissel***

Sécurité numérique
Annexe 07 du CCAP

SOMMAIRE

ARTICLE 1.- CLAUSES DE SECURITE NUMERIQUE.....	3
1.1. Préliminaires portant protection de l'information.....	3
1.2. Règles relatives au règlement général sur la protection des données.....	3
1.2.1. Généralités.....	3
1.2.2. Hébergement et accès aux données.....	3
1.2.3. Exigences de sécurité.....	3
1.3. Auto-contrôle du TITULAIRE.....	5
1.4. Incidents de sécurité.....	5
1.5. Sous-traitance.....	5
1.6. Transfert du Marché.....	6
2.1. Objet de la clause.....	6
2.2. Environnement de confiance – Qualification SecNumCloud.....	6
2.3. Fonctionnalités collaboratives obligatoires.....	6
2.4. Gestion des droits d'accès multi-entreprises.....	7
2.5. Conformité réglementaire et sécurité.....	7
2.6. Clauses de réversibilité.....	7

ARTICLE 1 - CLAUSES DE SECURITE NUMERIQUE

1.1 - Préliminaires portant protection de l'information

La mise en œuvre des présentes stipulations ne dispense pas de l'application des documents suivants :

- L'instruction générale interministérielle n° 1300/SGDSN/PSE/PSD du 9 août 2021 sur la protection du secret de la défense nationale (IGI 1300).
- L'instruction interministérielle n°901 (II 901) relative à la protection des systèmes d'information sensibles afférente aux informations « DIFFUSION RESTREINTE ».
- Le Règlement (UE) 2016/679 du parlement européen et 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 (règlement général sur la protection des données) dit RGPD.

1.2 - Règles relatives au règlement général sur la protection des données

1.2.1 - Généralités

Article 1.2.1.1 :

Le TITULAIRE confirme avoir pris connaissance des règles de sécurité à appliquer en signant le formulaire d'engagement et de reconnaissance de responsabilité joint en annexe (annexe 7b) du CCAP.

Article 1.2.1.2 :

Le TITULAIRE rédige au sein de son Offre un Plan d'Assurance Sécurité (PAS) joint en annexe de la consultation, qui deviendra contractuel à compter de la signature du Marché. Ce PAS précise les engagements du TITULAIRE pour répondre aux exigences de sécurité du Marché et les moyens qu'il mettra en œuvre pour assurer que les biens produits respectent les exigences de sécurité du Marché.

1.2.2 - Hébergement et accès aux données

Article 1.2.2.1 :

Le TITULAIRE a précisé dans son Offre les lieux géographiques dans lesquels les données informatiques liées à la prestation seront hébergées et conforme ce lieu à la signature du Marché. En cas de changement, le TITULAIRE devra prévenir dans les délais les plus contraints le MOA.

1.2.3 - Exigences de sécurité

Article 1.2.3.1 :

Les données du MOA, quel que soit leur support, sont strictement couvertes par le secret professionnel (article 226-13 du Code pénal). Le TITULAIRE s'engage à prendre toutes les

précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées.

- Le TITULAIRE s'engage donc à respecter, de façon absolue, les obligations suivantes et à les faire respecter par son personnel et/ou sous-traitants déclarés ou non :
- Ne prendre aucune copie des documents et supports d'informations confiés, à l'exception de celles nécessaires pour les besoins de l'exécution de sa prestation envers l'acheteur ;
- Ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées dans les prestations couvertes par le Marché remporté par le TITULAIRE ;
- Ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales ;
- Prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution du contrat ;
- Prendre toutes mesures, notamment de sécurité matérielle, pour assurer la conservation des documents et informations traités tout au long de la durée du présent contrat.

Il est rappelé qu'en cas de non-respect des dispositions précitées, la responsabilité du TITULAIRE peut également être engagée sur la base des dispositions des articles 226-17 et 226-5 du Code pénal.

Article 1.2.3.2 :

Le TITULAIRE reconnaît avoir fait signer par tous ses agents appelés sous sa responsabilité à un titre quelconque à intervenir pour le compte du TITULAIRE dans le cadre de l'exécution du Marché, une attestation de reconnaissance de responsabilité (Cf. annexe 7b) par laquelle lesdits agents attestent avoir pris connaissance des exigences et contraintes de sécurité imposées par le MOA, ainsi que de la législation applicable.

Article 1.2.3.3 :

Le TITULAIRE a l'obligation de communiquer au service bénéficiaire du Marché la liste de ses agents, que ceux-ci soient salariés du TITULAIRE ou salariés d'un de ses sous-traitants, susceptibles d'intervenir dans l'exécution du Marché. Tout changement dans la composition de cette liste doit être porté à la connaissance de cet organisme sans délai. À défaut, un état de lieux annuel de cette liste sera adressé à l'organisme bénéficiaire du Marché à la date anniversaire de la signature dudit Marché.

Article 1.2.3.4 :

Dans le cas où des informations sensibles, quelle que soit la forme de leur support, sont appelées à être conservées dans les locaux du TITULAIRE, leur support papier ou électronique doivent être disposées en dehors de leur utilisation dans des armoires fermant à clé et dont la clé est conservée par la seule personne responsable de leur utilisation.

Article 1.2.3.5 :

Le TITULAIRE conserve et traite les données du MOA de manière séparée de ses propres données ou de données d'autres clients du TITULAIRE. Le TITULAIRE doit restreindre l'accès aux données de l'acheteur suivant le principe de restriction au besoin d'en connaître.

Article 1.2.3.6 :

Le TITULAIRE garantit que les supports échangés ou à connecter sur un SI du MOA n'intègrent aucun code malveillant et ont fait l'objet d'un test d'innocuité positif au moyen d'une attestation à fournir au MOA.

Article 1.2.3.7 :

Le TITULAIRE ne tente pas d'accéder à des informations ou des ressources informatiques ne faisant pas partie du périmètre de la prestation.

Article 1.2.3.8 :

À la fin de la prestation, le TITULAIRE doit restituer les matériels fournis par le MOA (postes de travail, clefs USB, badge d'accès etc.)

Article 1.2.3.9 :

Le TITULAIRE est tenu de s'assurer d'une destruction effective des documents à l'issue du Marché ou en cas de perte d'utilité fonctionnelle de ceux-ci.

1.3 - Auto-contrôle du TITULAIRE**Article 1.3.1.1 :**

Le TITULAIRE effectue des autocontrôles de conformité aux exigences du Marché pour garantir et maintenir un niveau de sécurité adéquat durant toute la durée de la prestation. Ceux-ci doivent à minima être réalisés annuellement. Le TITULAIRE doit être en mesure d'apporter la preuve de ces autocontrôles sur demande du MOA.

1.4 - Incidents de sécurité**Article 1.4.1.1 :**

Le TITULAIRE, en cas de tentative d'intrusion sur ses systèmes d'information, à l'obligation d'en porter immédiatement connaissances aux services compétents du ministère de l'Intérieur à l'adresse suivante :

dzsn-zo@interieur.gouv.fr

1.5 - Sous-traitance**Article 1.5.1.1 :**

Les obligations du TITULAIRE, y compris les clauses de sécurités, s'appliquent intégralement à ses sous-traitants et sont sous sa responsabilité.

1.6 - Transfert du Marché

Article 1.6.1.1 :

Dans le cas d'une reprise du Marché, le nouveau TITULAIRE met en œuvre des mesures techniques et organisationnelles pour garantir la sécurité des données et des applications qui lui sont confiées, lors du transfert des prestations de la part du précédent TITULAIRE en conformité avec les réglementations applicables.

Le TITULAIRE initial veille donc à assurer l'ensemble des opérations pour que le nouveau TITULAIRE puisse reprendre l'exécution du Marché dans de bonnes conditions (transfert de compétences, documentations...). Durant la phase de transfert, l'assurance de la sécurité réside notamment dans :

- La gestion des accès et des habilitations ;
- Le transfert de responsabilités ;
- La fourniture d'informations nécessitant des mesures de protection adaptées ;
- La gestion de la continuité de l'activité.

Le TITULAIRE initial reste responsable de la sécurité jusqu'à la fin de la phase de transfert.

ARTICLE 2 - CLAUSES TECHNIQUES – GESTION MULTI-ENTREPRISES ET FONCTIONNALITES COLLABORATIVES SECURISEES

1.7 - Objet de la clause

La présente clause vise à définir les exigences fonctionnelles et techniques minimales que doit respecter la solution logicielle proposée dans le cadre du présent Marché. Celle-ci devra permettre la gestion sécurisée et collaborative des documents entre plusieurs entreprises au travers d'une solution labellisée **SecNumCloud**.

Pendant toute la durée d'exécution du présent Marché, l'ensemble des échanges de données, documents, informations ou fichiers entre le MOA et le TITULAIRE, ainsi qu'entre les différentes entreprises, devront obligatoirement transiter par la solution logicielle retenue, hébergée sur une infrastructure qualifiée SecNumCloud. Aucun échange de données relatives au Marché ne pourra se faire en dehors de ce canal sécurisé, sauf dérogation écrite préalable de l'acheteur.

1.8 - Environnement de confiance – Qualification SecNumCloud

La solution logicielle proposée devra disposer d'une qualification SecNumCloud valide, conformément aux exigences définies par l'ANSSI. Le TITULAIRE devra fournir les documents justificatifs suivants :

- Attestation de qualification SecNumCloud pour la solution utilisée ;
- Description du périmètre de la qualification ;
- Engagement sur le maintien de la qualification pendant toute la durée du Marché.

1.9 - Fonctionnalités collaboratives obligatoires

La solution devra obligatoirement proposer, au minimum, les fonctionnalités suivantes :

- Un espace collaboratif sécurisé pour les utilisateurs de différentes entités juridiques ;
- Le partage sécurisé de documents avec gestion fine des droits d'accès (lecture, écriture, commentaire) ;

- La possibilité d'ajouter des annotations en ligne directement sur les documents ;
- Un système de mémos ou de commentaires liés aux documents ;
- Le versionning complet des documents (avec traçabilité des modifications et restauration possible) ;
- Une fonctionnalité de signature électronique conforme au règlement eIDAS ;
- Un module de gestion d'agenda partagé avec notifications et droits d'accès différenciés.

1.10 - Gestion des droits d'accès multi-entreprises

Le TITULAIRE devra assurer la gestion des droits d'accès aux documents et à la solution logicielle conformément aux consignes et aux politiques définies par le MOA. Il s'engage à mettre en œuvre tous les mécanismes nécessaires pour garantir l'application rigoureuse des règles d'accès définies, notamment en ce qui concerne la confidentialité inter-entreprises, les droits spécifiques par profil, et l'auditabilité des modifications des droits.

Le TITULAIRE devra assurer la mise en œuvre d'un mécanisme de gestion des droits d'accès permettant :

- La distinction explicite des entités (entreprises) utilisatrices ;
- La gestion granulaire des droits par utilisateur, par groupe, et par organisation ;
- La traçabilité complète des accès et des actions (logs) ;
- La possibilité de délégation et d'administration déléguée par entreprise ;
- La conformité aux principes de sécurité Zero Trust et au RGPD.

1.11 - Conformité réglementaire et sécurité

La solution devra :

- Garantir la confidentialité, l'intégrité et la disponibilité des données ;
- Chiffrer les données en transit (TLS 1.2+) et au repos (AES-256 minimum) ;
- Être conforme au RGPD et permettre l'exercice des droits des personnes concernées ;
- Fournir un plan de reprise d'activité (PRA) et de continuité (PCA) avec des DIMA/PDMA (RTO/RPO) contractualisés ;
- Permettre l'auditabilité des accès et des actions réalisées sur les données.

1.12 - Clauses de réversibilité

À l'issue du Marché ou en cas de résiliation anticipée, le prestataire devra :

- Permettre l'export des données dans un format structuré, ouvert et interopérable (XML, JSON, etc.) ;
- Supprimer intégralement les données du système après restitution, avec remise d'un certificat de purge ;
- Fournir une documentation technique sur la structure des données exportées.