MINISTÈRE DE LA JUSTICE
Liberté
Égalité
Fraternité

Direction générale de l'administration pénitentiaire

CERTIFICAT DE CONFIDENTIALITE ET DE NON-DIVULGATION

A - Identification du pouvoir adjudicateur (ci-après « la DISP »)

Ministère de la Justice - Direction générale de l'administration pénitentiaire

DIRECTION DES SERVICES PÉNITENTIAIRES D'OUTRE-MER
48 Rue Denis Papin
94200 Ivry sur seine

CP BAIE-MAHAUT
12 Rue de la Manche à l'eau
97122 Baie-Mahaut

B - Identification de la société (ci-après « la Société »)

Nom de la société : ……

Adresse du siège : ……

……

Représentée par : ……

En qualité de : ……

C – Objet de la mission (ci-après « la mission »)

……

……

D – Informations confidentielles

Le terme « informations confidentielles » désigne les informations divulguées pendant toute la durée du présent accord par les parties, nonobstant le support sur lequel l'information a été communiquée. Ces informations concernent, de manière non limitative :

- Les données sources : plans, études, comptes-rendus, notes de calcul, schémas, documents et toute autre information concernant la sécurité pénitentiaire, et l'Établissement pénitentiaire / la Direction générale de l'administration pénitentiaire dans son ensemble.
- Les données traitées : données qui résultent de tout type de traitement des données-sources.

Les informations confidentielles concernent également les données à caractère personnel comme défini dans le Règlement n°2016-679 du 27 avril 2016 sur la protection des données.

Ne constituent pas des informations confidentielles les informations appartenant au domaine public, préalablement à la divulgation.

E – Les textes applicables

La Société doit se conformer aux textes suivants :

- Le Règlement n°2016-679 portant sur la protection des données personnelles
- L'Arrêté du 18 août 2016 portant approbation de la politique ministérielle de défense et de sécurité
- L'article 413-9 du Code Pénal

F – Les obligations de la Société

La Société s'engage à la plus stricte confidentialité à l'égard des données-sources qui lui seront transmises par la DISP et des données traitées qui en résulteront.

La Société s'engage notamment à :

- Utiliser exclusivement les informations confidentielles dans le cadre du marché public conclu entre les parties,
- Ne pas communiquer les informations confidentielles à un tiers sans l'accord écrit de la DISP. Le tiers concerné sera soumis aux mêmes règles de confidentialité incombant à la Société.
- Limiter l'utilisation des informations confidentielles, afin que la diffusion desdites informations au sein de son organisation ne concerne que les personnes qui y sont habilitées (voir et compléter le tableau ci-dessous),
- Informer tous les détenteurs des informations confidentielles que lesdites informations revêtent un caractère secret, et s'assurer que chaque détenteur remplit les conditions énoncées par le présent certificat.

La Société se porte garante de la bonne exécution de l'obligation de confidentialité par les personnes auxquelles elle aura communiqué l'information, notamment la Société se porte fort du respect de la présente déclaration par ses salariés, même après que ceux-ci auront cessé leurs fonctions, sachant que seuls les salariés habilités par la présente déclaration pourront avoir accès aux informations confidentielles.

La Société se porte également garante de la bonne exécution de l'obligation de confidentialité par tous tiers auxquels elle aura communiqué l'information, après accord écrit de la DSPOM, et qui ne seraient pas inscrits dans le tableau ci-dessous.

Pour ce faire :
La Société réceptionnera les données-sources dont elle a demandé communication via la plateforme France Transfert (France transfert) associée à la solution de chiffrement ZED.

La Société utilisera les données-sources et traitées pour le seul objet de la mission qui lui est confiée, et ne prendra aucune copie des documents et supports d'informations confiés, à l'exception de celles nécessaires pour les besoins de l'exécution de sa prestation, objet du présent marché.

Le tableau suivant doit être rempli exhaustivement ; la présente doit nous être retournée accompagnée de la copie des pièces d'identité visées (passeport, ou carte nationale d'identité RECTO-VERSO). L'autorisation d'accès aux données se fait selon le principe du moindre privilège, les accès sont individuels et incessibles. Les comptes techniques doivent être inventoriés.

Nom et prénom de la personne ayant accès aux données	Type de document d'identité communiqué à la DISP	Numéro de document d'identité

La Société ne communiquera à aucune autre personne, sous aucun prétexte, les données qui lui sont transmises.

Hébergements des données sensibles du ministère

La Société stockera les données (sources et traitées) soit chiffrées sur un ordinateur équipé d'une solution de chiffrement certifiée ANSSI, soit sur support physique déposé dans un coffre-fort homologué (quand elles ne sont pas utilisées par un personnel habilité ci-dessus). Le type de sécurisation choisi par la Société doit garantir le Ministère de la Justice contre tout accès par un tiers non autorisé, qu'il s'agisse d'un vol de support physique ou d'un piratage par des voies informatiques.

L'hébergement des données sensibles de la Direction générale de l'administration pénitentiaire sur le territoire national est obligatoire, sauf dérogation dûment motivée et précisée dans la décision d'homologation, ou accord du HFDS (Haut fonctionnaire de défense et de sécurité du Ministère de la Justice).

Seuls les systèmes d'information du ministère répondent aux exigences de la PSSI de l'Etat. L'usage de système de stockage en ligne tel que DropBox, skyDrive, Google drive, ou bien d'échanges tel que WeTransfer, SendBox, TransferNow, ne satisfaisant pas à ce prérequis, leur usage est prohibé. Ces règles s'appliquent également pour tout hébergement assuré par un partenaire privé pour le compte du ministère. Seuls les systèmes de stockage et partage suivants sont qualifiées ou en cours de qualification : OODrive, Orange Cloud for Business, Outscale SAS, Vendome Solutions. La liste à jour peut être retrouvée sur le site de l'ANSSI (Agence nationale de la sécurité des systèmes d'information). Cette liste peut rendre caduque les qualifications des solutions citées à titre d'exemple.

Destruction des données

La Société s'engage :

- À détruire en fin de mission **(à la fin de l'année de Garantie de parfait achèvement)** l'ensemble des supports physiques des données-sources et les données traitées.
- À effacer l'ensemble de ces données (sources et traitées) qui auraient pu être stockées sur ses ordinateurs, serveurs et tous matériels comportant un dispositif de mémoire.
- À s'assurer que son/ses sous-traitants dûment déclarés et agréés détruisent également les données-source et les données traitées, et collecter puis transmettre à la DSPOM les attestations sur l'honneur correspondantes (voir ci-dessous).

La Société renonce en conséquence à conserver toute trace des données (sources et traitées) manipulées dans le cadre de la présente mission, sous quelque format que ce soit (papier, informatique, maquette…). Ces données, sources et traitées, seront remises exclusivement au pouvoir adjudicateur.

La Société fournira en fin de mission à la Direction générale de l'administration pénitentiaire une attestation sur l'honneur de la parfaite et complète destruction de toutes ces données, par elle-même ainsi que par ses éventuels

sous-traitants (notamment les plans de l'Établissement Pénitentiaire), dans ses locaux ou sur ses serveurs et autres équipements de stockage.

Si la Société souhaite consulter ultérieurement le fruit de son travail, celui-ci sera à sa disposition sur demande au sein des locaux de la Direction interrégionale des services pénitentiaires de Toulouse.

La société est en revanche autorisée à faire état de la présente mission dans ses réponses à appels d'offres ultérieurs, sous réserve de ne communiquer aucune donnée sensible de sécurité pouvant mettre en péril la sécurité de l'Établissement pénitentiaire, à quelque personne que ce soit.

La Société devra informer sans délai la Direction générale de l'administration pénitentiaire de toute difficulté dans l'application de ces mesures, de fuite ou de suspicion de fuite d'informations sensibles qu'elle rencontre ou constate. Une attention particulière doit être portée à la conservation des preuves numériques relatives à cette information.

La DSPOM se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect des obligations précitées par un tiers qu'il aura préalablement agréé.

G – Durée du certificat

Le certificat entre en vigueur dès la signature de ce dernier par la Société, et est valable jusqu'à ce que la Société fournisse, à la fin de sa mission, l'attestation sur l'honneur de la parfaite et complète destruction de toutes les données confidentielles (données sources et données traitées) dans ses locaux ou sur ses serveurs et autres équipements de stockage.

La fin du certificat de confidentialité ne dégage pas la Société de ses obligations quant à l'utilisation, la protection et la non-divulgation des informations confidentielles communiquées pendant la mission.

H – Interdictions

Les Parties élaborent et signent le présent certificat intuitu personae. Il est interdit à la Société de céder le présent certificat à un tiers sans l'accord écrit de la DISP.

La Société ne peut décompiler, désassembler ou démonter les informations confidentielles sans l'accord exprès de la DISP.

I – Responsabilité

L'inexécution contractuelle d'une quelconque stipulation contenue dans le présent certificat engagera de plein droit la responsabilité de la Société, conformément au droit commun, qui se verra confrontée à des poursuites de la Direction générale de l'administration pénitentiaire.

La DSPOM pourra prononcer la résiliation immédiate du marché, sans indemnité en faveur du titulaire, en cas de violation du secret professionnel ou de non-respect des dispositions précitées.

J – Droit applicable

En cas de litige, seul le Tribunal Administratif du lieu de réalisation de l'ouvrage est compétent en la matière.

COMMENT FAIRE EN PRATIQUE :

Objectif = limiter les exfiltrations de données par des cyberattaquants

Pour respecter les engagements de confidentialité, il faut concrètement :

- Échanger les fichiers entre DISP et la Société, avec l'outil France Transfert, chiffrés avec l'outil ZED (avec mot de passe transmis à part : SMS, mail)
- Une fois reçus par l'entreprise, il faut :
    - Sécuriser les fichiers en conservant le chiffrement ZED, ou bien mettre dans un coffre-fort physique si des impressions sont nécessaires pour travailler
    - Donner accès seulement aux personnes ayant besoin d'en connaître pour la prestation demandée
    - Sortir les fichiers du coffre (ZED ou physique) le temps nécessaire, sans jamais laisser les fichiers accessibles par un tiers (verrouiller le PC), puis remettre les données au coffre dès que plus besoin de travailler sur les fichiers
- En fin d'opération, détruire les données-sources et les données traitées
- S'assurer de faire appliquer les mêmes règles aux sous-traitants éventuels

Attestation à retourner par la Société

Je m'engage, en pleine connaissance de cause, à respecter les clauses ci-dessus.

Nom + qualité du signataire : ……

Date : ……

Signature + cachet de la société