

**CONTRAT DE MAINTENANCE DU LOGICIEL GESTION ENFANCE 3D OUEST
ET SERVICES ASSOCIÉS**
Prise d'effet au 01/01/2022

ENTRE LES SOUSSIGNÉ(E)S

La Société 3D OUEST

Dont le Siège social est situé 5 rue de Broglie, 22300 LANNION
représentée légalement par Monsieur DELOUARD Jean-Michel,
Directeur de 3D OUEST
Ci-après dénommée « **LE PRESTATAIRE** » (Sous-traitant)
D'une part,

Acte 042-214200750-20220407-2022-23-DE Numéro 2022-23 Date de décision 07/04/2022 Nature DE Objet Contrat de maintenance du logiciel enfance Classification 1.4 - Autres types de contrats

ET

CRAINTILLEUX

place Jean Dussurgey 42210 CRAINTILLEUX
représenté légalement par Madame, Monsieur Le Maire
Ci après dénommé « **LE CLIENT** » (Responsable des traitements)
D'autre part,

IL A ÉTÉ ARRÊTÉ ET CONVENU CE QUI SUIT

PREAMBULE

L'entreprise 3D OUEST est le concepteur du logiciel «GESTION ENFANCE 3D OUEST» et le présent contrat de maintenance s'inscrit dans la continuité de l'utilisation du logiciel acquis par :

Madame, Monsieur Le Maire de CRAINTILLEUX,

Le logiciel «GESTION ENFANCE 3D OUEST», est soumis aux termes et aux conditions énumérées dans le présent contrat de maintenance et son annexe I RGPD.

ARTICLE 1er - OBJET

Le présent contrat a pour objet la prise en charge de l'entretien et de la maintenance du logiciel «GESTION ENFANCE 3D OUEST».

Le prestataire connaît parfaitement le logiciel à l'exception de l'environnement informatique qui devra lui être indiqué. Par suivi et maintenance, les parties entendent que le prestataire réalisera les prestations suivantes :

- assistance téléphonique
- déblocage du logiciel
- mise à disposition des nouvelles versions
- intégration des mises à jour
- hébergement et sauvegarde des données
- assistance téléphonique des administrés (lorsque ce service a été souscrit)
- accompagnement, mission pour le compte de la collectivité (lorsque ce service a été souscrit).

Ne sont pas comprises dans la maintenance définie ci-dessus, les dépenses diverses et le matériel nécessaire pour la réparation des dommages subis par le client, si ces dommages résultent notamment d'une mauvaise utilisation, d'une utilisation abusive du logiciel ou d'une négligence de la part du client, d'une installation électrique défectueuse, de la foudre, du non-respect des instructions d'exploitation, d'une intervention sur le logiciel effectuée par un tiers non agréé

expressément par le prestataire ainsi que tout dommage résultant de l'emploi de fournitures et matériels non agréés, de la force majeure ou du fait du tiers.

En tout état de cause, la responsabilité du prestataire est limitée aux obligations contractuelles définies au terme du présent contrat.

Les prestations d'entretien et de maintenance seront exécutées avec la diligence nécessaire pour limiter l'impact sur le fonctionnement des services du client.

Le terme « mises à jour » désigne ici toute évolution logicielle intégrant des fonctionnalités additionnelles, des améliorations mineures ou la correction de bogues.

Le prestataire s'engage à maintenir le logiciel de telle manière que le client dispose des correctifs et mises à jour lui permettant de répondre à ses besoins opérationnels.

Le prestataire n'est pas tenu de fournir au client des services d'assistance technique, autres que ceux stipulés dans le cadre du présent contrat de maintenance.

ARTICLE 2 - OBLIGATIONS DU CLIENT

Le client doit assurer au prestataire toute facilité pour l'exécution de sa prestation.

De manière générale, le client devra apporter tout son concours au prestataire dans l'exécution de sa prestation et s'engage à collaborer afin de permettre au mieux la réalisation des prestations dues.

Le client s'oblige à fournir au prestataire les coordonnées d'un interlocuteur technique, qui puisse être contacté par téléphone ou par mail pour faciliter l'identification et la résolution du problème.

ARTICLE 3 – NATURE DES PRESTATIONS

Les prestations réalisées par le prestataire peuvent être de deux natures :

- celles fournies au titre de la redevance annuelle forfaitaire et décrites dans le cadre du présent contrat,
- celles fournies en option et rémunérées selon un tarif défini sur devis et accepté par le client.

ARTICLE 4 – PRESTATIONS REMUNEREES FORFAITAIEMENT

4.1.- Assistance à l'utilisateur

Cette assistance consiste à fournir à l'utilisateur, par téléphone, les explications dont il a besoin pour utiliser les fonctionnalités du logiciel.

Ce service est accessible au client sur appel de sa part dans les conditions décrites à l'article 10 - PROCÉDURE D'INTERVENTION.

Le client devra mettre en œuvre les recommandations formulées par le service d'assistance.

Dans le cadre du présent contrat, le temps d'assistance téléphonique consacré par le prestataire au client est plafonné à deux heures par mois. Le temps non utilisé pourra être cumulé pour répondre à un besoin ponctuel plus important.

En cas de dépassement récurrent de ce plafond d'heures, la prestation d'assistance à l'utilisateur pourra faire l'objet d'une facturation au cas par cas sur la base d'un tarif négocié avec le client en fonction de la nature du problème constaté.

4.2.- Maintenance corrective

Dans le cadre de cette intervention, le prestataire assurera la correction du code informatique à l'origine d'anomalies dans le fonctionnement du logiciel. Il pourra ponctuellement recourir à une solution de contournement pour permettre la continuité des activités du client.

Seule sera prise en compte l'anomalie de fonctionnement clairement décrite par le client et reproductible.

Dans ce cadre et par tous les moyens qui sont à sa disposition (télémaintenance, téléphone, etc.), le prestataire pourra solliciter l'assistance du client pour caractériser précisément l'anomalie et être en mesure de la résoudre au plus vite.

Une anomalie non bloquante ne permet pas au client l'exploitation complète du logiciel. Certaines fonctionnalités peuvent être dégradées. L'anomalie ne présente pas un caractère critique.

Une anomalie bloquante ne permet pas au client l'exploitation des fonctionnalités majeures du logiciel. L'anomalie présente un caractère critique.

4.3.- Mises à jour

Le prestataire pourra réaliser durant le temps du contrat de maintenance des mises à jour du logiciel. Les plus importantes donneront lieu à une information préalable sur le portail de connexion ou par l'envoi de mails aux utilisateurs.

On entend par « mises à jour » : l'ajout ou la modification de fonctionnalités, la correction d'anomalies, des améliorations concernant la rapidité d'exécution, des évolutions relatives à l'ergonomie et la facilité d'utilisation.

Cela comprend la mise à jour de la documentation et des tutoriaux en ligne.

Les évolutions logicielles définies ci-dessus seront mises en ligne par le prestataire selon une périodicité dont ce dernier reste seul juge.

4.4.- Maintenance évolutive

Le prestataire réalisera les maintenances évolutives nécessaires pour prendre en compte les nouvelles prescriptions légales ou les changements de réglementation.

Cette maintenance comprend l'intégration de fonctionnalités permettant de faire face aux évolutions juridiques de l'environnement logiciel (ex : recommandations de la CNIL / obligations relatives au RGPD).

4.5.- Maintenance préventive

Le prestataire réalisera à intervalles réguliers une maintenance préventive sur ses logiciels afin d'anticiper et pallier d'éventuels dysfonctionnements pouvant avoir pour origine des évolutions diverses de l'environnement technique général (ex : nouvelle version de navigateur internet).

Cette maintenance préventive pourra donner lieu à des interruptions ponctuelles de services. En tout état de cause, ces dernières seront réalisées, chaque fois que c'est possible, aux heures ayant le moins d'impact possible pour les utilisateurs. Elles feront l'objet par ailleurs d'une information préalable aux utilisateurs.

ARTICLE 5 – PRESTATIONS OPTIONNELLES

Le prestataire pourra proposer à titre onéreux des journées d'analyse et de développement afin de pallier une éventuelle montée en charge non prévue par le client lors de l'acquisition ou l'ajout de fonctionnalités spécifiques demandées par celui-ci.

Le prestataire peut également assurer à titre onéreux des séances de formation complémentaire ou d'accompagnement en ligne ou sur site.

ARTICLE 6 - PRIX

Le client devra régler au prestataire une redevance forfaitaire annuelle telle que prévue à la signature du bon de commande pour la première année. Ensuite elle sera revue selon le paragraphe « Révision des prix » ci-dessous.

Des aménagements pourront avoir lieu, avec l'accord du client, pour qu'à l'issue de la première année de maintenance, il soit facturé une maintenance depuis la date anniversaire jusqu'au 31 décembre de la même année. Cela permettant, par la suite, une facturation du 1er janvier au 31 décembre de chaque année.

Les interventions conséquentes nécessitées pour un usage non conforme aux prestations d'utilisation du logiciel ou par une défectuosité non imputable au prestataire donneront lieu à une facturation distincte selon le tarif en vigueur.

Toute maintenance relative à un développement spécifique connexe pourra faire l'objet d'un avenant au présent contrat.

La licence en vigueur au profit du client, ainsi que toutes les garanties, conditions, exclusions et limitations de responsabilités aux termes du contrat, s'appliqueront aux mises à jour effectuées pendant la période comprise entre la date d'acquisition de la licence et la date d'expiration de la maintenance contractée par le client.

Le prestataire mettra à la disposition du client les mises à jour disponibles et l'informerá des évolutions intervenues.

Révision des prix

Le prix de la maintenance sera révisé annuellement selon une formule qui prend en compte l'indice Syntec :

$$P_n = P_0 \times (I_n / I_0)$$

P_n = prix après révision,

P_0 = prix avant révision,

I_n = indice de l'année de maintenance N^* ,

I_0 = indice de l'année de la maintenance $N-1^{**}$.

** I_n = indice de l'année de maintenance connu au 01/01/ N*

*** I_0 = indice utilisé lors de la précédente révision, ou pour les acquisitions en cours d'année l'indice retenu sera l'indice connu au 01/01 après la date d'achat.*

ARTICLE 7 – DUREE ET RESILIATION

Sauf dans le cadre d'un marché spécifique, le contrat de maintenance est prévu pour une durée de douze mois. Il est renouvelable annuellement par tacite reconduction dans la limite de 4 ans.

Dans le cas où le client ne souhaiterait plus bénéficier du contrat de maintenance, la personne habilitée devra avertir le prestataire, au moins deux mois avant la date d'expiration de la période en cours par courrier en recommandé.

Dans le cadre de la portabilité des données, le client résiliant le contrat de maintenance se verra remettre à la date de fin de maintenance l'ensemble de ses données sur un support approprié.

A la demande expresse du client, le prestataire pourra conserver 6 mois le contenu de la base de données en vue de pallier toute fausse manipulation durant cette période.

Suite à une période de résiliation, un nouveau contrat de maintenance pourra être souscrit, et cela sans pénalité sous réserve que les évolutions intervenues sur le logiciel ou le format des données à réintégrer ne nécessitent pas d'adaptations notables.

Si tel devait être le cas, un devis sera proposé au client pour réintégrer ses données.

ARTICLE 8 – PROPRIETE

Le prestataire assure avoir pris toutes les précautions d'usage pour la préservation des données.

Dans le cas où le prestataire venait à disparaître (cession ou liquidation), les données seront restituées au client.

Le client reste le propriétaire de toutes les données dont il aura confié le traitement au prestataire.

Le prestataire, quant à lui, pourra seul prétendre à la propriété des développements informatiques.

ARTICLE 9 - SECRET ET CONFIDENTIALITE

Chacune des parties s'engage à garder comme confidentiels les informations et les documents quels qu'ils soient (statistiques, codes confidentiels, informations économiques, techniques, commerciales, etc.) dont elles ont eu accès au cours de l'exécution du contrat.

Les deux parties prendront, vis-à-vis de leurs personnels et de leurs prestataires toutes les mesures nécessaires pour assurer sous leurs responsabilités la confidentialité de toutes les informations et documents visés à l'alinéa ci-dessus.

ARTICLE 10 – PROCEDURE D'INTERVENTION

10.1.- Heures et délais d'intervention

Les interventions du prestataire s'effectuent dans une plage hebdomadaire allant du lundi au vendredi et des horaires allant de 8H30 à 12H00 et de 14H00 à 18H00 au numéro de téléphone suivant: 02 96 48 68 19.

A la demande du client, ces limites pourront être étendues dans le cadre d'un avenant au présent contrat et après acceptation d'un devis.

Les demandes d'intervention seront prises en compte dans les meilleurs délais lors des jours ouvrés. Faisant suite au signalement d'un incident, le client pourra être tenu informé du temps nécessaire pour corriger le dysfonctionnement.

Le prestataire mettra en œuvre tous les moyens à sa disposition pour corriger le problème rencontré et cela dans les 24 heures s'agissant d'un problème bloquant et dans les 72 heures dans le cas d'un problème non bloquant sauf conditions particulières définies préalablement.

10.2. - Modalités de l'intervention

Le client détermine un interlocuteur unique et un suppléant pour toutes demandes d'assistance et d'intervention. Celui-ci formulera sa demande en précisant clairement la nature de son besoin.

Il décrira celle-ci de telle façon que le prestataire puisse caractériser l'incident au plus vite.

L'information du prestataire se fera par téléphone ou par messagerie électronique (contact@3douest.com ou celle de l'interlocuteur habituel).

ARTICLE 11 - HEBERGEMENT DES APPLICATIONS ET DES DONNEES

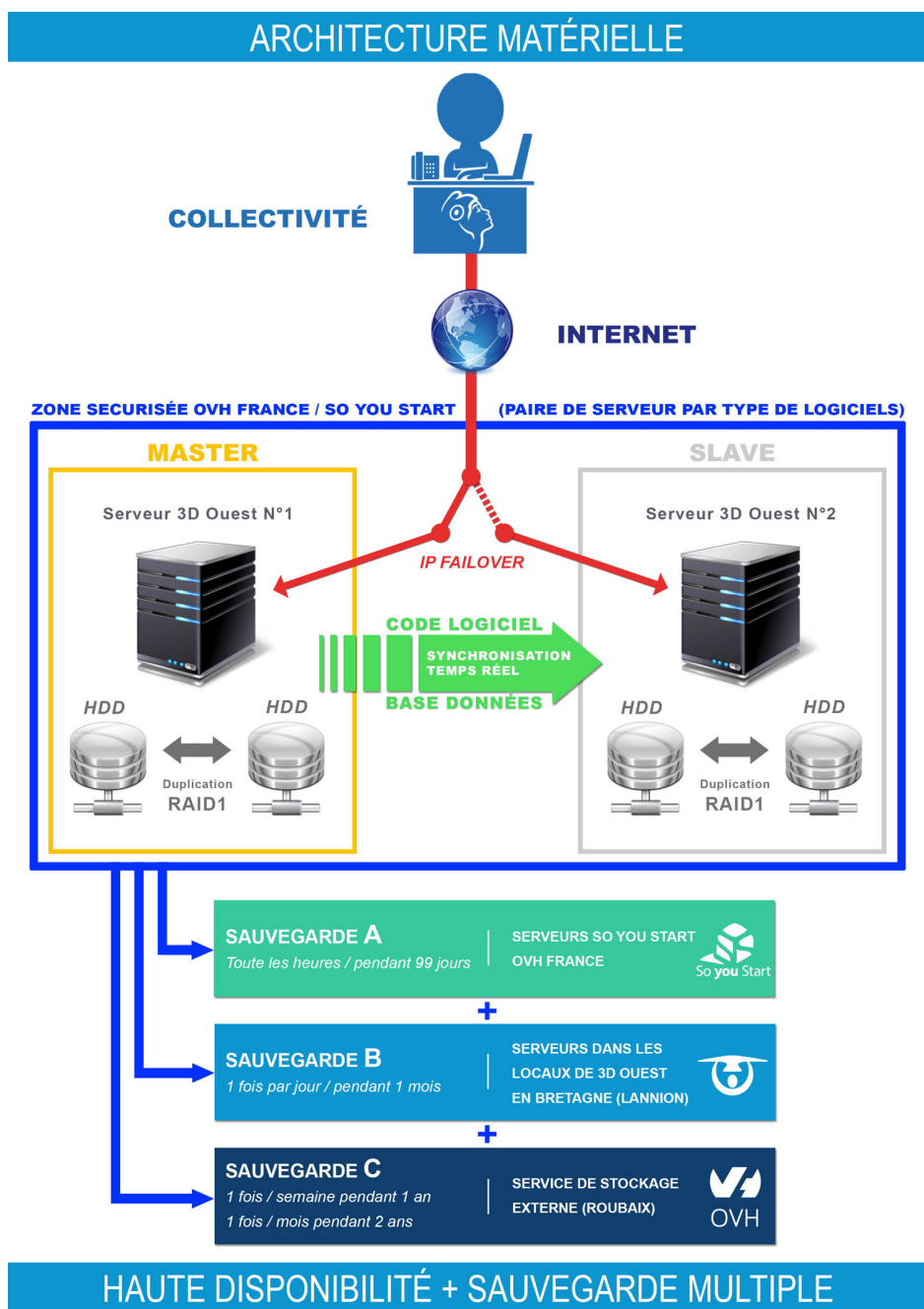
11.1 - Généralités

Les solutions techniques mises en œuvre par 3D OUEST ont pour objectif d'assurer un fonctionnement robuste de l'application, garantissant de fait une continuité du service pour le Client.
L'application est mutualisée entre les clients utilisateurs, permettant des évolutions optimales et simultanées pour tous les utilisateurs d'une même application.

Pour des raisons de sécurité et de confidentialité des données, chaque client dispose d'une base de données personnelle (en dehors des cas particuliers nécessitant la mutualisation des données entre plusieurs infrastructures).

11.2 - Architecture

L'architecture des serveurs hébergeant la solution logicielle se présente ainsi :



Le prestataire dispose d'une architecture basée sur des paires de serveurs (Master et Slave) associés à chaque type d'application logicielle.

Ces machines sont équipées par 3D OUEST d'un dispositif de réplication en temps réel du code et des données (Master sur Slave) et d'une fonction IP FAILOVER assurant le basculement semi-automatique du Master vers le Slave.

Cela permet une disponibilité permanente de l'application en cas d'arrêt ou défaillance du serveur principal (Master) sans risque de perte de données.

Chaque serveur dispose également de son propre système de réplication de données (Raid 1) grâce à 2 disques durs par machine.

11.3 - Matériel

Les machines utilisées sont des serveurs de la gamme OVH et SO YOU START.

Elles sont situées exclusivement sur le territoire français et présentent les caractéristiques suivantes :

- Processeur : Intel Xeon E3 12.25 - 4c/4t - 3.2 GHz - 8 Mo SmartCache
- Mémoire RAM : 32 Go DDR3
- Disque Dur : 2 x 2To - SATA2

Ces serveurs physiques disposent de distributions Linux standard avec Firewall logiciel ainsi que de serveurs logiciels Apache (Web) et MySQL (Bases de données).

L'ouverture des ports est faite en fonction des nécessités de fonctionnement de l'application de gestion.

Par défaut, seuls les ports suivants sont laissés ouverts :

- 80 - http
- 443 - https
- 22 - ssh

Selon les besoins du client, d'autres ports peuvent être ouverts pour permettre des actions spécifiques.

L'accès distant en ssh n'est possible que par clés RSA privées/publiques.

Les requêtes Ping sont autorisées.

Un Pare-feu est présent sur chaque serveur.

L'hébergement est fait dans les Datacenters d'OVH dont les locaux sont sécurisés (alimentation électrique redondante, lutte contre les incendies, climatisation, etc.).

Seules les personnes habilitées au sein d'OVH peuvent y pénétrer et accéder physiquement aux serveurs pour remédier aux problèmes techniques rencontrés (matériel - système - réseau).

Le prestataire assure le monitoring de ses serveurs à distance et est informé en permanence de chacune des interventions sur le matériel.

La plate-forme est également sécurisée contre les attaques extérieures (pare-feu, système de détection d'intrusion, application des correctifs de sécurité à jour, méthodologie et outils de développements choisis pour développer la solution, etc.).

Les choix techniques définis ici sont susceptibles d'évoluer pendant la durée du contrat de maintenance pour répondre

aux contraintes de performance et de sécurité.

11.4 - Sécurité des accès au logiciel

L'accès des utilisateurs de l'application se fait par login et mot de passe en passant par un service d'authentification.

Chaque connexion (back office, front office) est conservée dans la base de données.

Tous les utilisateurs enregistrés peuvent changer de mot de passe.

Pour renforcer la sécurité, il est possible de limiter l'accès du Back Office à un certain nombre de postes (adresses IP) définies par avance.

11.5 - Sauvegarde des données

Les données sont sauvegardées régulièrement sur différents sites, permettant une restauration complète et cohérente en cas de panne ou de toute autre défaillance.

Le plan de sauvegarde permet de sauvegarder les bases de données sur les 99 derniers jours.

Au-delà de 99 jours, une sauvegarde par semaine est conservée.

Une sauvegarde quotidienne supplémentaire est également effectuée sur un serveur distant sur le territoire national.

11.6 - Disponibilité du service

La solution proposée est utilisable et accessible 7 jours sur 7 et 24 heures sur 24.

Le prestataire teste l'accès à la page de connexion toutes les 5 minutes et un mail est automatiquement renvoyé au support en cas de problème.

Si la collectivité a besoin de réinjecter des données sauvegardées, elle devra contacter 3D OUEST et préciser quelle sauvegarde devra être importée (date et heure).

Le prestataire se chargera alors de mettre à jour la base de données avec la sauvegarde concernée.

11.7 - Portabilité

Le client est réputé « producteur » de la base de données au sens de l'article L341-1 du code de la propriété intellectuelle. Il détient par conséquent les droits de propriété afférents à la base de données. A ce titre, il dispose de celle-ci comme bon lui semble.

Le prestataire s'engage à ne pas utiliser, copier, extraire des données, reproduire, représenter, diffuser, en tout ou en partie, par quelque moyen que ce soit et à quelque personne que ce soit, la base de données ou toute copie, même partielle, pendant la durée d'exécution du contrat de maintenance et à l'issue de celui-ci.

La restitution des données ou « portabilité » fait partie intégrante de la prestation d'hébergement. À tout moment, et dans tous les cas à la fin du marché, le client pourra demander au prestataire de mettre en œuvre une prestation d'extraction de l'ensemble des données en ligne et archivées.

11.8 - Disponibilité

Les délais exprimés dans le tableau ci-dessous sont des maximums. Le prestataire essaiera toujours de les réduire pour offrir la meilleure qualité de service.

Plage de disponibilité de la solution proposée (7j/7,24h/24)	7j/7 - 24h/24
Durée annuelle maximale d'indisponibilité non planifiée durant la plage d'utilisation de la solution proposée	12 heures
Durée maximale d'une indisponibilité immédiate non planifiée durant la plage d'utilisation de la solution proposée (temps de rétablissement de service)	1 heure
Durée annuelle maximale d'indisponibilité planifiée durant la plage d'utilisation de la solution proposée (arrêts planifiés pour contraintes d'exploitation)	5 heures
Délai de latence maximal du service en ligne (réponse au ping)	0,5 s
Délai maximal d'affichage de la page d'accueil de l'application Backoffice après identification de l'utilisateur	3 secondes
Délai maximal d'affichage de la page d'accueil de l'application FrontOffice après identification de l'utilisateur (administré ou client)	3 secondes
Délai maximal d'affichage d'une page d'affichage suite à une recherche multicritères	10 secondes
<u>Réversibilité</u> Délai de restitution des données mise en ligne et archivées par le prestataire pour la personne publique	2 jours ouvrés

ARTICLE 12 - COMMUNICATION

Le prestataire est autorisé à informer par mail le client de toutes évolutions ou services associés concernant le logiciel dont il a l'usage.

Le client fera savoir au prestataire s'il s'oppose à l'utilisation de son logo dans le cadre d'une démarche de référencement clients.

ARTICLE 13 - CONCLUSION

L'offre de maintenance est expressément limitée aux termes des articles du présent contrat de maintenance et de son Annexe I RGPD.

Celles-ci seront interprétées et régies conformément au droit français.

Tous les litiges, difficultés et réclamations relatifs à l'interprétation et à l'exécution des conditions générales de maintenance seront soumis aux tribunaux compétents.

Aucune modification, suppression ou addition au présent contrat ne pourra être apportée sans l'accord écrit des deux parties. Ces éventuelles modifications prendront effet à la date de signature de l'avenant au présent contrat ou à une date spécifiée sur celui-ci.

Si une ou plusieurs stipulations du contrat sont tenues pour non valides ou déclarées telles en application d'une Loi, d'un règlement ou à la suite d'une décision définitive d'une juridiction compétente, les autres stipulations du contrat garderont toute leur force et leur portée.

Les parties conviendront alors de remplacer la clause déclarée nulle et non valide par une clause qui se rapprochera le plus quant à son contenu de la clause initialement arrêtée.

ANNEXE I

CONDITIONS DE MAINTENANCE RELATIVES AU RGPD (Règlement Général sur la Protection des Données) *Entrant en application à partir du 25 mai 2018*

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le sous-traitant (PRESTATAIRE) s'engage à effectuer pour le compte du responsable des traitements (CLIENT) les opérations de traitement de données à caractère personnel.

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.

I. Description du traitement faisant l'objet de la sous-traitance

Le sous-traitant (PRESTATAIRE) est autorisé à traiter pour le compte du responsable des traitements (CLIENT) les données à caractère personnel nécessaires pour fournir les services de maintenance et tierce maintenance applicative.

Ces prestations permettent le maintien en condition opérationnelle des matériels et/ou logiciels à titre préventif, correctif ou évolutif.

*Par **préventif**, on entend les mesures d'entretien exécutées pour éviter la survenance d'anomalies.*

*Par **correctif**, on entend les mesures consistant à corriger les anomalies.*

*Par **évolutif**, on entend les mesures de maintenance visant à faire évoluer ou à adapter une ou plusieurs applications, afin d'intégrer de nouvelles fonctions, d'en améliorer le fonctionnement ou de prendre en compte de nouvelles dispositions législatives ou réglementaires.*

*Par **tierce maintenance applicative**, on désigne les prestations qui consistent à conserver un programme informatique dans un état lui permettant de remplir sa fonction.*

Les opérations réalisées sur les données peuvent porter sur les :

- Traitements liés à la consultation
- Traitements relatifs à la création ou la modification
- Traitements d'import et d'export
- Traitements de sauvegarde ou de restauration
- Traitements de sécurisation : chiffrement-déchiffrement, pseudonymisation
- Traitement d'archivage, d'anonymisation ou de suppression
- Traitements de récupération et de nettoyage
- Divers autres usages liés aux obligations de maintenance

La finalité du traitement a pour objectif d'optimiser les opérations administratives, comptables et organisationnelles du responsable de traitement (CLIENT) dans le cadre de l'exercice de son métier ou de ses missions. Elle porte également sur la génération de statistiques.

Les données à caractère personnel traitées se limitent à ce qui est nécessaire pour répondre aux besoins du responsable du traitement (CLIENT).

Les catégories de personnes concernées par les différentes étapes du traitement des données à caractère personnel

sont les agents chargés du support logiciel, les intégrateurs de données, les développeurs informatiques et les administrateurs réseaux qui sont rattachés au type de logiciel métier mis en place par le sous-traitant (PRESTATAIRE).

Pour l'exécution du service objet du présent contrat, le responsable de traitement (CLIENT) met à la disposition du sous-traitant (PRESTATAIRE) les informations nécessaires suivantes :

- La liste, les qualifications et les informations de contact des personnels de la Collectivité intervenant dans le processus de maintenance,
- Le cas échéant la liste, les qualifications et les informations de contact des personnels des autres sous-traitants de la Collectivité intervenant dans le processus de maintenance,
- Toutes les procédures, codes d'accès, moyens techniques ou physiques et tout autre document utile pour permettre l'exécution des services objet du contrat dans les meilleures conditions (télémaintenance, prise en main à distance, documentations techniques, etc.),
- L'accès aux règlements de la Collectivité.

II. Obligations du sous-traitant (PRESTATAIRE) vis-à-vis du responsable de traitement (CLIENT)

Le sous-traitant (PRESTATAIRE) s'engage à :

- Traiter les données uniquement pour les seules finalités qui font l'objet de la sous-traitance.
- Traiter les données conformément aux instructions du responsable de traitement (CLIENT).

Nota : Si le sous-traitant (PRESTATAIRE) 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 (CLIENT).

- Garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent contrat.
- Veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent contrat :
 - S'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
 - Soient sensibilisées 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**.

III. Conditions de Sous-traitance

Le sous-traitant (PRESTATAIRE) peut faire appel à un autre sous-traitant (ci-après nommé « **le sous-traitant ultérieur** ») pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le responsable de traitement de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance.

Le responsable de traitement (CLIENT) dispose d'un délai de 10 jours ouvrés à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le responsable de traitement n'a pas émis d'objection pendant le délai convenu.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du responsable de traitement. Il appartient au sous-traitant (PRESTATAIRE) initial de s'assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement européen sur la protection des données.

Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant (PRESTATAIRE) initial demeure pleinement responsable devant le responsable de traitement de l'exécution par l'autre sous-traitant de ses obligations.

IV. Droit d'information des personnes concernées

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

V. Exercice des droits des personnes

Dans la mesure du possible, le sous-traitant (PRESTATAIRE) aidera le responsable de traitement (CLIENT) à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

Lorsque les personnes concernées exercent auprès du sous-traitant (PRESTATAIRE) des demandes d'exercice de leurs droits, le sous-traitant (PRESTATAIRE) doit transmettre ces demandes dès réception par courrier électronique à l'adresse du DPO (Data Protection Officer) du responsable des traitements (CLIENT). Ses coordonnées sont à préciser en fin de document.

VI. Notification des violations de données à caractère personnel

Le sous-traitant (PRESTATAIRE) notifie au responsable de traitement (CLIENT) toute violation de données à caractère personnel dans un délai maximum de 4 heures après en avoir pris connaissance. Il le fera par courrier électronique à l'adresse du DPO du responsable des traitements (CLIENT) précisé en fin de document.

Cette notification est accompagnée de toute documentation utile afin de permettre au responsable de traitement (CLIENT), si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

Après accord du responsable de traitement, le sous-traitant (PRESTATAIRE) notifiera à l'autorité de contrôle compétente (la CNIL), au nom et pour le compte du responsable de traitement, les violations de données à caractère personnel dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, 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 le responsable du traitement (CLIENT) 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.

S'il n'est pas possible de fournir toutes ces informations en même temps, elles pourront être communiquées de manière échelonnée mais sans retard indu.

Après accord du responsable des traitement (CLIENT), le sous-traitant (PRESTATAIRE) 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

VII. Aide du sous-traitant au responsable de traitement pour le respect de ses obligations

Le sous-traitant (PRESTATAIRE) aide le responsable de traitement pour la réalisation d'analyses d'impact relatives à la protection des données.

Le sous-traitant (PRESTATAIRE) aide le responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle.

VIII. Mesures de sécurité

Le sous-traitant (PRESTATAIRE) s'engage à mettre en œuvre les mesures techniques et organisationnelles garantissant un niveau de sécurité adapté au risque, y compris, entre autres :

- La « **pseudonymisation** » et le **chiffrement** des données à caractère personnel.
- Les moyens garantissant la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services des traitements.
- 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.
- La sécurité physique des locaux : Protection contre les menaces incendie & dégâts des eaux, protection des matériels contre les pertes de services essentiels (groupes électrogènes, onduleurs, parafoudre, double adduction courant fort & courant faible, etc.), protection contre les intrusions, contrôle des accès, gestion et suivi des habilitations d'accès incluant la gestion des visiteurs, procédures d'alertes sur incidents.
- La sécurité organisationnelle : Responsabilités en matière de sécurité formellement définies et affectées, sensibilisation des personnels à la sécurité des données, processus d'habilitation des accès aux systèmes d'information traitant des données, procédure de gestion et notification des incidents de sécurité ou des demandes contraignantes affectant les données, Plan de Continuité d'Activité (PCA), Plan de Secours Informatique (PSI), organisation de gestion de crise.
- La sécurité logique : Durcissement des environnements informatiques, procédure de gestion des correctifs de sécurité, cloisonnement des architectures réseau (VLAN, DMZ) et filtrage (firewalls), sondes anti intrusions, contrôle d'accès par authentification, politique de mots de passe, protection des environnements informatiques sensibles par logiciel antivirus à jour (programmes et bases de signatures virales).
- La sécurisation des flux d'échanges de données à caractère personnel (chiffrement, authentification), de manière à ce qu'ils ne puissent être exploités par un tiers non autorisé.
- La traçabilité des actions et la gestion des preuves : Conservation des traces d'audit des activités sur le

système informatique (accès utilisateurs, accès et actions administrateurs, changements des paramètres de sécurité des systèmes, accès aux données à caractère personnel, etc.), horodatage fiable des traces d'audit, durée de conservation des traces garantie (à minima un an sauf contrainte réglementaire).

- La mise en place de procédures de contrôle pour s'assurer du maintien du niveau de sécurité dans le temps (tests d'intrusion, scans de vulnérabilité, test de charge, audits internes de sécurité, veille de sécurité).

Le sous-traitant (PRESTATAIRE) s'engage à mettre en œuvre toutes les mesures de sécurité prévues par les textes et recommandations en vigueur dans notre contexte public : notamment le RGS Référentiel Général de Sécurité et les recommandations de l'ANSSI.

Ces mesures s'appliquent dès lors que le sous-traitant agit avec des moyens humains et techniques placés sous sa responsabilité qui ne dépendent pas directement de la Collectivité (infrastructures, INTERNET, personnels, etc.).

IX. Sort des données

Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s'engage à renvoyer toutes les données à caractère personnel au responsable de traitement.

Le renvoi s'accompagnera de la destruction de toutes les copies existantes dans les systèmes d'information du sous-traitant et de tous les acteurs éventuels de la chaîne de sous-traitance sous sa responsabilité.

Le sous-traitant (PRESTATAIRE) pourra justifier par écrit, à la demande du responsable des données (CLIENT), de la destruction effective des données.

X. Délégué à la protection des données

Le sous-traitant (PRESTATAIRE) communique au responsable de traitement (CLIENT) **le nom et les coordonnées de son délégué à la protection des données**, s'il en a désigné un, conformément à l'article 37 du règlement européen sur la protection des données (voir fin du document).

XI. Registre des catégories d'activités de traitement

Le sous-traitant (PRESTATAIRE) déclare **tenir par écrit un registre** de toutes les catégories d'activités de traitement effectuées pour le compte du responsable de traitement comprenant :

- Le nom et les coordonnées du responsable des traitements (CLIENT) pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données.
- Les catégories de traitements effectués pour le compte du responsable des traitements (CLIENT).
- 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 européen sur la protection des données, les documents attestant de l'existence de garanties appropriées.
- Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, 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.

XII. Documentation

Le sous-traitant (PRESTATAIRE) 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.

Nota : *S'agissant du recueil d'informations portant sur la sécurité même des systèmes et infrastructures du sous-traitant (PRESTATAIRE), les auditeurs externes (entreprises privées) désignés par le responsable des données (CLIENT) feront l'objet d'une enquête préalable par les services du sous-traitant (PRESTATAIRE) avant de pouvoir procéder à tout audit technique.*

Cette enquête aura pour objectif de vérifier la probité de l'auditeur et l'absence de conflit d'intérêt.

XIII. Obligations du responsable de traitement (CLIENT) vis-à-vis du sous-traitant (PRESTATAIRE)

Le responsable de traitement (CLIENT) s'engage à :

- Fournir au sous-traitant (PRESTATAIRE) les informations visées au I des présentes clauses.
- Documenter par écrit toute instruction concernant le traitement des données par le sous-traitant (PRESTATAIRE).
- 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 sous-traitant (PRESTATAIRE).
- Superviser le traitement, y compris réaliser le cas échéant les audits et les inspections auprès du sous-traitant (PRESTATAIRE).

Le responsable des traitements (CLIENT) reconnaît avoir connaissance de l'ensemble des fonctionnalités mises à sa disposition par le sous-traitant (PRESTATAIRE) au moment de la mise en place de l'application.

Le sous-traitant (PRESTATAIRE) s'engage de son côté à l'informer de toute nouvelle fonctionnalité jouant un rôle dans le traitement des données à caractère personnel.

Le responsable du traitement (CLIENT) prend l'engagement à ne pas faire usage, ni détourner les fonctionnalités du logiciel pour réaliser des actions sortant du strict cadre pour lequel l'application a été conçue.

Le sous-traitant (PRESTATAIRE) ne saurait être tenu responsable de l'usage fait, hors du cadre du RGPD, par le responsable des traitement (CLIENT) des fonctionnalités dont dispose le logiciel et notamment de :

- L'envoi de mails ou sms à caractère publicitaire sans le consentement préalable du tiers,
- L'envoi de mails ou sms relatifs à un sujet sans rapport avec l'objectif initial du logiciel,
- L'usage des champs divers pour l'enregistrement de données à caractère personnel et ou sensible sans rapport avec l'objectif initial du logiciel,
- L'enregistrement et le stockage de fichiers et documents comportant des informations dépassant le domaine objet du traitement réalisé par le logiciel,
- Les sauvegardes de bases de données et export (Excel, Pdf, ...) faits à partir du logiciel.

XIV. Informations à compléter par le sous-traitant (PRESTATAIRE)

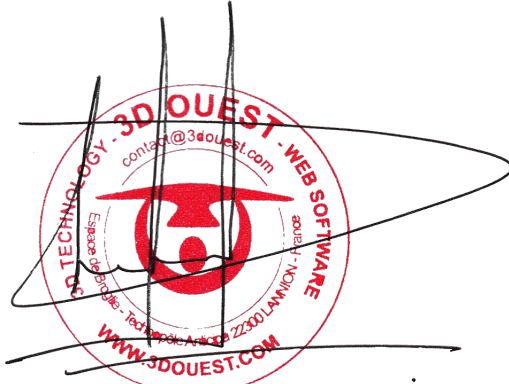
Nom et prénom du DPO	DELATTRE Laurent
Son adresse professionnelle	3D OUEST - 5 rue Louis de Broglie – 22300 LANNION (France)
Son numéro de téléphone professionnel	02 56 66 20 07
Son Email professionnel	dpo@3douest.com

XV. Informations à compléter par le responsable des traitements (CLIENT)

Nom et prénom du DPO (ou à défaut du CIL)	
Son adresse professionnelle	
Son numéro de téléphone professionnel	
Son Email professionnel	

Fait à Lannion

En deux exemplaires originaux pour chacune des parties

<p>Pour 3D OUEST Jean-Michel DELOUARD Directeur</p> 	<p>Pour le Client Signature et qualité du responsable</p> <p>Penser à compléter les informations relatives à votre DPO (article XV ci-dessus)</p>
--	---